有限群论基础

王萼芳 编著

清华大学出版社

目　　录

第一章 基本概念

群论的研究起源于十八世纪末，它是由于方程式论的需要，首先作为置换群的理论而发展起来的。随后，发现在大多数问题中，重要的不是构成群的置换本身，而应注意的是一个集合在代数运算下的性质，因而提出了一般群的概念。一般群论的建立，不仅扩大了群论研究的对象和应用，而且还可以从各种不同的群得到多方面的启发，从而丰富了群论研究的方法，促进了群论的发展。

这一章介绍群的定义和一些基本概念，并在§2中详细介绍了置换和置换群的概念，作为进一步研究一般群和置换群的基础。

§1 群的概念

1.1 群的定义

定义1 设G是一个非空集合，在G中定义了一种代数运算，称为乘法，记作“·”，即对于G中任意两个元素a，b，都唯一确定G中一个元素$a\cdot b$，称为a，b的**乘积**。如果G对这种运算满足下面几个条件：

1) **结合律** 对G中任意三个元素a，b，c，都有

$$(a\cdot b)\cdot c=a\cdot(b\cdot c).$$

2) **单位元素的存在** G中存在一个元素e，对于G中任意元素a，都有

$$e\cdot a=a\cdot e=a.$$

3) **逆元素的存在** 对于G中任一个元素a，都可找到G中一个元素a^{-1}，使得

$$a^{-1}\cdot a=a\cdot a^{-1}=e,$$

那么G就称为一个**群**。元素e称为G的**单位元素**，a^{-1}称为a的**逆元素**。

定义2 如果群G还满足

4) **交换律** 对于G中任意两个元素a，b，都有

$$a\cdot b=b\cdot a,$$

那么G就称作一个**交换群**或**阿贝尔群**。

如果群G的运算不满足交换律，则称G为**非交换群**。

为了简便起见，在不致混淆的情况下，我们常用ab表示a与b的乘积。

有时候，有些交换群的运算用加法表示，记作“+”，$a+b$称为a与b的和。那么条件1)—4)就成为

1′) **结合律** 对G中任意三个元素a，b，c，都有

$$(a+b)+c=a+(b+c).$$

2′) **零元素的存在** G中存在一个元素0，对于G中任一个元素a，都有

$$0+a=a+0=a.$$

3′) **负元素的存在** 对于G中任一个元素a，都可找到G中一个元素$-a$，使得

$$(-a)+a=a+(-a)=0.$$

4′) **交换律** 对于G中任意两个元素a，b，都有

$$a+b=b+a.$$

0称为G的**零元素**，$-a$称为a的**负元素**。

1.2 群的例子

例1 全体整数所成的集合Z对于数的加法成一交换群，因为Z对数的加法满足条件1′)—4′).群Z的零元素就是整数0，整数n的负元素就是$-n$。

同样地，全体有理数所成集合Q,全体实数所成集合R，全体复数所成集合C，对于数的加法也都成为交换群。

例2 全体非零有理数Q^*，全体非零实数R^*，全体非零复数C^*对数的乘法都构成交换群。

但是全体非零整数对数的乘法不成为群，因为不满足条件3)。全体正整数对数的加法也不成为群，因为不满足条件2)及3)。

例3 n是一个正整数。全部n次单位根所成集合U_n对于数的乘法组成一个交换群。

例4 用$M_n(R)$表示全部n级可逆实矩阵所成的集合。$M_n(R)$对矩阵的乘法构成一个群。当$n\geqslant 2$时，这个群是非交换的。

例5 用$L_n(R)$表示n维实向量空间$R^{(n)}$的全部可逆线性变换所成的集合。$L_n(R)$对变换的乘法构成群。当$n\geqslant 2$时，这个群是非交换的。

例6 设F是一个域，F对F的加法成为一个交换群。F中非零元素的集合F^*对F的乘法也成为一个交换群。

例7 设V是域P上一个线性空间。V对向量的加法成一个交换群。

例8 $G=\{a,b,c,d\}$。用下列乘法表定义G的运算：

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

表中第i行第j列处的元素表示左边的第i个元素与表上边第j个元素之积。例如，上表说明

$$a\cdot a=a,\ b\cdot c=d,$$

等等。请读者自己验证G对这个运算构成一个交换群。

用乘法表来给出一个群是常常用到的方法，我们在以后还会遇到。

1.3 简单性质

从群的定义，可以推出下面一些性质。

1) 群中只有一个单位元素。

证明 设G是一个群，e是G的单位元素。如果e'也是G的单位元素，那么，因为e是单位元素，所以

$$e\cdot e'=e'.$$

又因e'也是单位元素，所以

$$e\cdot e'=e.$$

因此，必须有

$$e'=e.$$

所以G的单位元素是唯一的。▎

2) 在群中，每个元素只有一个逆元素。

证明 设a是群G中的一个元素，e是G的单位元素，a^{-1}是a的逆元素。如果a'也是a的逆元素，那么，根据逆

元素的定义，有

$$(a' \cdot a)a^{-1} = e \cdot a^{-1} = a^{-1},$$

$$a' \cdot (a \cdot a^{-1}) = a' \cdot e = a'.$$

由结合律，即得

$$a' = a^{-1}.$$

所以逆元素是唯一的。 ▎

由逆元素的唯一性，可得

3） $(a^{-1})^{-1} = a$。

4）群中消去律成立，即

如果 $ab = ac$，**则有** $b = c$。**如果** $ba = ca$，**则有** $b = c$。

证明 设 $ab = ac$。

用 a^{-1} 左乘等式两端，得

$$a^{-1}(ab) = a^{-1}(ac).$$

于是 $$(a^{-1}a)b = (a^{-1}a)c.$$

从而

$$eb = ec, \quad b = c.$$

同样可证第二个等式。 ▎

5）在群中，对于任意两个元素 a，b，**方程**

$$ax = b \text{ 及 } ya = b$$

都有解，而且解是唯一的。

证明 显然，元素 $a^{-1}b$ 及 ba^{-1} 分别是这两个方程的解，解的唯一性可由消去律得出。 ▎

需要注意的是，因为群中交换律不一定成立，所以上面两个方程的解一般是不相等的，只有在 a 与 b 可交换，即 $ab = ba$ 时，这两个解才相等。

对于群中一个元素 a，我们把 $n(n>0)$ 个 a 相乘所得的元素记作 a^n，即

$$\underbrace{a \cdot a \cdot \cdots \cdot a}_{n\text{个}} = a^n.$$

对于负整数 $-n$ $(n>0)$，规定

$$a^{-n} = (a^{-1})^n,$$

并约定 a^0 表示群的单位元素。a^n（n 为任意整数）称为 a 的**方幂**。根据结合律，可知

6）群中指数律成立，即

$$a^n \cdot a^m = a^{n+m}, \quad n, m \text{ 为任意整数；}$$

$$(a^n)^m = a^{nm}, \quad n, m \text{ 为任意整数。}$$

如果 $ab = ba$，**则有**

$$(ab)^n = a^n b^n, \quad n \text{ 为任意整数。}$$

如果所讨论的群是交换群，而且群的运算用加法表示，那么上面的一些性质可以叙述为：

1′）群中只有一个零元素。

2′）在群中，每个元素只有一个零元素。

3′） $-(-a) = a$。

以后，常用 $a - b$ 表示 $a + (-b)$。

4′）如果 $a + b = a + c$，**则有** $b = c$。

5′）对于任意两个元素 a, b，**方程**

$$a + x = b$$

有唯一解 $x = b - a$。

对于加法交换群来说，一个元素的方幂就是这个元素的**倍数**。当 $n>0$ 时，我们用 na 表示 n 个 a 相加所得之和：

$$\underbrace{a + a + \cdots + a}_{n\text{个}} = na.$$

规定

$$(-n)a = -(na),$$

并约定 $0a$ 表示群的零元素。于是下列倍数律成立：

6′） $na+ma=(n+m)a$，　n,m 为任意整数；

$m(na)=mna$，　n,m 为任意整数；

$n(a+b)=na+nb$，　n 为任意整数。

1.4 阶

定义3 如果群 G 包含的元素个数有限，则称 G 为**有限群**。否则称 G 为**无限群**。有限群 G 所包含的元素个数称为 G **的阶**。

我们常常用 $|G|$ 表示有限群 G 的阶。

定义4 设 a 是群 G 中一个元素，如果存在正整数 k 使得 $a^k=e$，则 a 称为**有限阶元素**。满足 $a^k=e$ 的最小正整数 k 叫做 a **的阶**。如果不存在正整数 k 使得 $a^k=e$，则 a 称为**无限阶元素**。

定义中的条件 $a^k=e$ 在加法群时应改为 $ka=e$。以后在讨论时我们往往只对乘法群来叙述，而对加法群的情形就不另外说明了。

例如，例1至例8中，例3中的群的阶等于 n；例7中的群的阶等于4；其余的群都是无限群。如果用 F_p 表示由 p 个元素构成的有限域，那么 F_p 的加法群是一个 p 阶交换群；而乘法群 F_p^* 是一个 $p-1$ 阶交换群。

在例1中除去零元素的阶等于1外，其它元素都是无限阶元素。在例8中，单位元素 a 是1阶元素，其它元素的阶都等于2。

从定义可以看出，在一个群中，单位元素(零元素，如果是加法群)是唯一的一个1阶元素。

我们以后主要讨论有限群。有限群中的元素一定都是有限阶元素。这个事实可以这样来证明，设 a 是有限群 G 中一个元素。考虑下列元素

$$a,a^2,a^3,\cdots.$$

由于 G 是一个有限群，所以这些元素中一定有相同的。即有正整数 $k_1<k_2$，使得

$$a^{k_1}=a^{k_2}.$$

于是
$$a^{k_2-k_1}=e,\quad k_2-k_1>0.$$

根据定义，a 是一个有限阶元素。

如果一个群中的所有元素都是有限阶元素，那么这个群称为**周期群**。有限群一定是周期群。

关于元素的阶有下述重要性质。

定理1 如果 a 是群 G 的一个 k 阶元素，e 是 G 的单位元素。那么

1） $a^l=e \rightleftharpoons k|l$.

2） $a^l=a^m \rightleftharpoons k|l-m$.

如果 a 是一个无限阶元素，那么

$$a^l=a^m \rightleftharpoons l=m.$$

证明 1）如果 $k|l$，那么可设 $l=kd$，d 是一个整数。于是

$$a^l=a^{kd}=(a^k)^d=e^d=e.$$

反之，如果 $k\nmid l$，可设

$$l=kd+r,\quad 0<r<k.$$

于是

$$a^l=a^{kd+r}=a^{kd}\cdot a^r=e\cdot a^r=a^r\neq e.$$

2）因为
$$a^l=a^m \rightleftharpoons a^{l-m}=e,$$

故由1)即得

$$a^l=a^m \rightleftharpoons k|l-m.$$

关于无限阶元素的结论可以从定义直接得到。❙

§2 置换群

置换群是一类最重要的有限群。作为群的例子，这一节介绍置换及置换群的概念。

2.1 置换及对称群

设Ω是由 n 个文字组成的集合：

$$\Omega=\{a_1,a_2,\cdots,a_n\}。$$

Ω 到自身的一个一一映射称为**(作用于)Ω 上的一个置换**，或 **n 元置换**，简称**置换**。有时候也称为 $a_1,a_2,\cdots,a_n$ 的一个置换。

设 σ 是 $\Omega=\{a_1,a_2,\cdots,a_n\}$ 上的一个置换。用a_i^σ $(i=1,2,\cdots,n)$表示 a_i 在 σ 下的象，而把 σ 表成

$$\sigma=\begin{pmatrix}a_1 & a_2 & \cdots & a_n\\ a_1^\sigma & a_2^\sigma & \cdots & a_n^\sigma\end{pmatrix}.$$

或者可以简单地表成

$$\sigma=\begin{pmatrix}a_i\\ a_i^\sigma\end{pmatrix}.$$

为了简单起见，有时常用 $1,2,\cdots,n$ 表示Ω 的 n 个元素，此时，σ 就可表成

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ 1^\sigma & 2^\sigma & \cdots & n^\sigma\end{pmatrix}=\begin{pmatrix}i\\ i^\sigma\end{pmatrix}.$$

因为 σ 是一个一一映射，所以 $1^\sigma,2^\sigma,\cdots,n^\sigma$ 是 $1,2,\cdots,n$ 的一个排列。两个不同的置换 σ,τ 所对应的排列$1^\sigma,2^\sigma,\cdots,n^\sigma$ 与 $1^\tau,2^\tau,\cdots,n^\tau$ 是不同的。而且，任给 $1,2,\cdots,n$ 的一个排列 $a_1,a_2,\cdots,a_n$。都有唯一的一个置换 σ 使得

$$i^\sigma=a_i,\quad i=1,2,\cdots,n.$$

即

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ a_1 & a_2 & \cdots & a_n\end{pmatrix}.$$

我们知道 n 元排列一共有 $n!$个。所以一共有 $n!$个 **n元置换**。我们用 S_n 表示这 $n!$个 n 元置换所成的集合。例如，一共有 6 个 3 元置换：

$$\sigma_1=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix},\quad \sigma_2=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix},$$

$$\sigma_3=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix},\quad \sigma_4=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix},$$

$$\sigma_5=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix},\quad \sigma_6=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}.$$

$S_3=\{\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5,\sigma_6\}$包含 6 个元素。

在 S_n 中可以按照映射的乘法定义运算。设 σ,τ 是$1,2,\cdots,n$ 的两个置换。那么我们规定 σ 与 τ 的乘积 $\sigma\tau$ 为将 σ，τ 连续作用。即

$$i^{\sigma\tau}=(i^\sigma)^\tau,\quad i=1,2,\cdots,n.$$

例如，4 元置换

$$\sigma=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 1 & 3\end{pmatrix}\text{与 }\tau=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}$$

的乘积为

$$\sigma\tau=\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}.$$

置换的乘法有下述一些性质。

1）满足结合律

$$(\sigma\tau)\rho=\sigma(\tau\rho),\quad \forall\,\sigma,\tau,\rho\in S_n.$$

2）n 元恒等置换

$$e=\begin{pmatrix}1&2&\cdots&n\\1&2&\cdots&n\end{pmatrix}$$

是 S_n 的单位元素

$$e\sigma=\sigma e=\sigma,\quad \forall\,\sigma\in S_n.$$

3）每个 n 元置换在 S_n 中都有逆元素

$$\begin{pmatrix}1&2&\cdots&n\\a_1&a_2&\cdots&a_n\end{pmatrix}^{-1}=\begin{pmatrix}a_1&a_2&\cdots&a_n\\1&2&\cdots&n\end{pmatrix}.$$

因此，我们有

定理2 n 元置换全体组成的集合 S_n 对置换的乘法构成一个群，称为 **n元对称群**，其阶为 $n!$。

需要注意的是，当 $n\geqslant3$ 时，S_n 是非交换的。例如对上面例子中的 σ,τ，就有

$$\tau\sigma=\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}\neq\sigma\tau.$$

例1 $S_2=\left\{e,\begin{pmatrix}1&2\\2&1\end{pmatrix}\right\}$是一个 2 阶交换群。

例2 $S_3=\{\sigma_1=e,\sigma_2,\sigma_3,\sigma_4,\sigma_5,\sigma_6\}$（$\sigma_i$ 如前）是一个 6 阶非交换群。S_3 的运算可以用下列乘法表给出：

	e	σ_2	σ_3	σ_4	σ_5	σ_6
e	e	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	e	σ_6	σ_5	σ_4	σ_3
σ_3	σ_3	σ_5	e	σ_6	σ_2	σ_4
σ_4	σ_4	σ_6	σ_5	e	σ_3	σ_2
σ_5	σ_5	σ_3	σ_4	σ_2	σ_6	e
σ_6	σ_6	σ_4	σ_2	σ_3	e	σ_5

2.2 置换的轮换表法

这一小节介绍置换的轮换表法。

首先看几个例子。在 S_3 中，σ_5将 1 映到 2， 2 映到 3，3 映到 1，我们将它表成(1,2,3)；σ_2 将 1 保持不变，将 2 映到 3， 3 映到 2，我们将它表成(1)(2,3)，或简单地表成(2,3)。

一般地，如果 n 元置换 σ 把 n 个文字中的一部分 $a_1,a_2,\cdots,a_m(m\leqslant n)$作如下变换：

$$a_1^\sigma=a_2,\quad a_2^\sigma=a_3,\quad\cdots,\quad a_{m-1}^\sigma=a_m,\quad a_m^\sigma=a_1,$$

而把其余 $n-m$ 个文字保持不变，则称 σ 为一个 **m-轮换**，**简称轮换**。记作

$$\sigma=(a_1,a_2,\cdots,a_m).$$

m 称为轮换 σ 的**长度**。当 $m=1$时，σ 就是恒等置换。当 $m=2$ 时，σ 只把两个文字互换，而保持其余的文字不变，称为一个**对换**。显然有

$$(a_1,a_2,\cdots,a_m)=(a_i,a_{i+1},\cdots,a_m,a_1,\cdots,a_{i-1}),\quad 1<i\leqslant m.$$

两个轮换 $\sigma=(a_1,a_2,\cdots,a_m)$与 $\tau=(\beta_1,\beta_2,\cdots,\beta_l)$称为

不相交的，如果 $\alpha_1,\alpha_2,\cdots,\alpha_m$ 与 $\beta_1,\beta_2,\cdots,\beta_l$ 是各不相同的。

很容易看出，不相交的轮换是可交换的。

定理3 任何一个置换都可表成一些不相交的轮换的乘积，而且表法(除轮换的次序外)是唯一的。

证明 设 σ 是 $1,2,\cdots,n$ 的一个置换。任取 $1,2,\cdots,n$ 中的一个，设为 α。作序列

$$\alpha=\alpha^{\sigma^0},\alpha^{\sigma},\alpha^{\sigma^2},\cdots.$$

因为

$$\alpha^{\sigma^k}\in\{1,2,\cdots,n\}\quad(k=0,1,2,\cdots).$$

因此这个序列一定包含重复的文字。设 α^{σ^m} 是其中第一个在前面出现过的文字，并设它与 α^{σ^i} $(0\leqslant i<m)$ 相同。于是 α，$\alpha^{\sigma},\cdots,\alpha^{\sigma^{m-1}}$ 各不相同。如果 $i\neq 0$。那么由

$$\alpha^{\sigma^i}=\alpha^{m}$$

可推出

$$(\alpha^{\sigma^{i-1}})^{\sigma}=(\alpha^{\sigma^{m-1}})^{\sigma}.$$

即 σ 将两个不同的文字 $\alpha^{\sigma^{i-1}}$ 与 $\alpha^{\sigma^{m-1}}$ 映到相同的文字，这是不可能的。所以 $i=0$，即 $\alpha^{\sigma^m}=\alpha$。作轮换

$$\sigma_1=(\alpha,\alpha^{\sigma},\cdots,\alpha^{\sigma^m}).$$

则 σ 与 σ_1 在 $\alpha,\alpha^{\sigma},\cdots,\alpha^{\sigma^{m-1}}$ 上的作用相同。

如果 $m=n$，那么 $\sigma=\sigma_1$ 是一个轮换。如果 $m<n$，在 $1,2,\cdots,n$ 中去掉 $\alpha,\alpha^{\sigma},\cdots,\alpha^{\sigma^{m-1}}$ 后，在剩下的文字中任取一个 β。仿照上面的方法可以得到一个轮换

$$\sigma_2=(\beta,\beta^{\sigma},\cdots,\beta^{\sigma^{r-1}}),$$

σ 与 σ_2 在 $\beta,\beta^{\sigma},\cdots,\beta^{\sigma^{r-1}}$ 上的作用相同。因为 σ 是一一映射，所以 σ_1 与 σ_2 不相交。

这样继续下去，直到 $1,2,\cdots,n$ 用完为止。我们就得到一些不相交的轮换 $\sigma_1,\sigma_2,\cdots,\sigma_s$，使

$$\sigma=\sigma_1\sigma_2\cdots\sigma_s.$$

表法的唯一性是很明显的。▎

例3

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8\\3&1&5&4&2&8&7&6\end{pmatrix}$$

$$=(1,3,5,2)(4)(6,8)(7).$$

置换的这种表法称为置换的**轮换表法**。如果在置换 σ 的轮换表法中，α 是一个文字组成一个轮换，那么 $\alpha^{\sigma}=\alpha$，即 σ 保持 α 不变。为了简单起见，在轮换表法中可以把这样的轮换省略不写。这种简单的表法，称为 σ 的**轮换表法的省略形式**。例如，例3中 σ 的轮换表法的省略形式为

$$(1,3,5,2)(6,8).$$

恒等置换保持每个文字都不变，我们可以任取一个文字把它表成一个1-轮换。不过，通常我们总是用 e 表示恒等置换。

应用置换的轮换表法，可以很容易计算置换的阶。一个长度为 l 的轮换的阶为 l。一般地，如果 σ 的轮换表法是

$$\sigma=\sigma_1\sigma_2\cdots\sigma_s,$$

其中 σ_i 的长度为 $l_i(i=1,2,\cdots,s)$，那么 σ 的阶等于 $l_1,l_2,\cdots,l_s$ 的最小公倍数 $[l_1,l_2,\cdots,l_s]$。下面我们来证明这个结论。

设 σ 的阶为 d。记 $[l_1,l_2,\cdots,l_s]=m$。则因

$$\sigma^m=\sigma_1^m\sigma_2^m\cdots\sigma_s^m=e,$$

所以

$$d\mid m.$$

另一方面，因为

$$\sigma^d=\sigma_1^d\sigma_2^d\cdots\sigma_s^d=e,$$

而 $\sigma_1^d, \sigma_2^d, \cdots, \sigma_s^d$ 无公共文字，故

$$\sigma_1^d = \sigma_2^d = \cdots = \sigma_s^d = e.$$

因此

$$l_i \mid d, \quad i = 1, 2, \cdots, s.$$

由最小公倍数的性质，知 $m \mid d$。

所以

$$d = m.$$

例4 试求置换

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 8 & 6 & 9 & 1 & 12 & 10 & 4 & 5 & 7 & 3 & 11 \end{pmatrix}$$

的阶。

解 因为 σ 的轮换表法为

$$(1,2,8,4,9,5)(3,6,12,11)(7,10),$$

所以 σ 的阶等于12。

置换的轮换表法有许多方便的地方，读者将在以后遇到轮换表法的一些应用。

2.3 置换的奇偶性 交错群

因为每个轮换都可表成一些对换的乘积：

$$(a_1, a_2, \cdots, a_m) = (a_1, a_2)(a_1, a_3)\cdots(a_1, a_m),$$

因此，每个置换也都可以表成对换的乘积。但是，一个置换表成对换的乘积的方法不是唯一的。例如

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = (1,2,3)(4,5)$$

$$= (1,2)(1,3)(4,5) = (2,3)(1,2)(4,5)$$

$$= (2,3)(1,2)(1,3)(4,5)(1,3).$$

然而，我们可以证明下述定理。

定理4 n元置换σ表成对换的乘积后，乘积中对换个数的奇偶由σ唯一确定，而且与 n 元排列$1^\sigma, 2^\sigma, \cdots, n^\sigma$的奇偶一致。

证明 设σ表成m个对换的乘积：

$$\sigma = \sigma_1\sigma_2\cdots\sigma_m.$$

我们来证明m的奇偶与 n 元排列$1^\sigma, 2^\sigma, \cdots, n^\sigma$ 的奇偶一致。σ将排列$1, 2, \cdots, n$ 变成排列 $1^\sigma, 2^\sigma, \cdots, n^\sigma$。因此将$m$个对换$\sigma_1, \sigma_2, \cdots, \sigma_m$依次连续作用于排列$1, 2, \cdots, n$也得到排列 $1^\sigma, 2^\sigma, \cdots, n^\sigma$。我们知道对换改变排列的奇偶，所以作$m$次对换就将排列的奇偶改变$m$次。由于$1, 2, \cdots, n$是一个偶排列，所以排列 $1^\sigma, 2^\sigma, \cdots, n^\sigma$ 的奇偶与m一致。因此m的奇偶由σ唯一确定。▎

根据这个定理，我们可以定义置换的奇偶性。

定义4 如果 n 元置换σ可以表成奇数个对换的乘积，则称σ为**奇置换**；如果σ可以表成偶数个对换的乘积，则称σ为**偶置换**。

由定义可知：如果 $1^\sigma, 2^\sigma, \cdots, n^\sigma$ 是一个奇排列，则σ是一个奇置换；如果$1^\sigma, 2^\sigma\cdots, n^\sigma$ 是一个偶排列，则σ是一个偶置换。

从定义还知，在$n!$个 n 元置换中，奇、偶置换的个数相同，各有$\frac{n!}{2}$个。恒等置换是偶置换。两个偶置换之积是偶置换。偶置换的逆置换也是偶置换。

定理5 n 元偶置换全体对置换的乘法构成一个群，其阶为 $n!/2$。

以后我们用 A_n 表示全部 n 元偶置换所成的群，称为 **n 元交错群**。

2.4 置 换 群

由 n 元置换组成的群称为 **n 元置换群**，简称 **置换群**。

例如，n 元对称群及 n 元交错群都是 n 元置换群。我们还可举出一些例子，这些例子在以后的讨论中还会用到。

例5 $G=\{e,(1,2,3),(1,3,2)\}$ 是一个 3 元置换群，它的阶等于 3。

例6 $G=\{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$ 是一个 4 阶 4 元置换群。

例7 $G=\{e,(1,2),(3,4),(1,2)(3,4),(1,3)(2,4),$

$$(1,4)(2,3),(1,3,2,4),(1,4,2,3)\}$$

是一个 8 阶 4 元置换群。

例8 仅由恒等置换组成的群也是一个置换群。

为了确切起见，我们称一个置换实际变动的文字个数为这个置换的**次数**。而称一个置换群所实际变动的文字个数为这个群的**次数**。例如，$(1,2,3)$ 可以说是一个 3 元置换，也可以说是一个 4 元置换，等等，但是它是一个 3 次置换。又如，例 5 中的置换群可以看成 3 元置换群、4 元置换群等，但是它是一个 3 次置换群。

置换群的计算在代数学中占有很重要的地位。给定了一个正整数 n 以后，决定全部 n 次置换群是置换群理论中一个重要的问题。当$n\leqslant 11$时，n 次置换群已经全部找出，而当n较大时，只能找出一些具有特殊性质的 n 次置换群，有关这方面的一些结果将在以后再进行介绍。

§3 子 群

3.1 定义及例

定义5 G是一个群，如果G的一个子集H对G的运算构成一个群，则称H是G的一个**子群**。如果G的子群H不等于G，则称H是G的一个**真子群**。

我们用$H\leqslant G$（或$G\geqslant H$）表示H是G的子群，用 $H<G$（或$G>H$）表示H是G的真子群。

任何一个群G都有两个明显的子群，一个是由一个单位元素组成的子群$\{e\}$，称为G的**单位子群**。还有一个就是G本身。这两个子群称为G的**平凡子群**，其余的子群(如果存在的话)称为**非平凡子群**。

下面再来看一些例子。

例1 由全部偶数组成的集合对数的加法组成一个群，是加法群$\boldsymbol{Z}$的一个子群。

例2 复数加群$\boldsymbol{C}$以实数加群$\boldsymbol{R}$，有理数加群$\boldsymbol{Q}$及整数加群$\boldsymbol{Z}$为真子群：

$$\boldsymbol{C}>\boldsymbol{R}>\boldsymbol{Q}>\boldsymbol{Z}.$$

例3 关于非零复数所成的乘法群也有类似的结果：

$$\boldsymbol{C}^*>\boldsymbol{R}^*>\boldsymbol{Q}^*.$$

例4 行列式等于 1 的 n 级实矩阵全体对矩阵的乘法组成一个群，是 n 级可逆实矩阵群$M_n(R)$ 的一个真子群。

例5 n 元交错群A_n是 n 元对称群的一个真子群。

例6 任一个 n 元置换群都是 n 元对称群的子群。

需要注意的是，G 的子群H不只是一个包含在 G 中的群，而且H的运算必须与G的运算一样。例如，乘法群$\boldsymbol{R}^*$不能看成加法群 $\boldsymbol{R}$的子群。

因为群G的子群H的运算与G的运算一样，所以H的单位元素就是G的单位元素。H中任一元素 a 在H中的逆元素也就是 a 在G中的逆元素。

3.2 判别条件

群G的一个子集H满足什么条件才能成为G的一个子群呢？我们来分析群G的子集H对G的运算是一个群的条件。首先H必须是非空的。其次，如果a,b在H中，那么它们的乘积必须也在H中，即H对G的运算是封闭的。下面再来考察群的三个条件。因为H包含在G中，所以结合律当然成立，这一条可以不必检验。由于子群的单位元素即群的单位元素，子群中元素的逆元素就是它在群中的逆元素。所以只要检查G的单位元素及H中元素的逆元素是否在H中。而且从H中元素的逆元素在H中以及H对运算的封闭性可以推出单位元素在H中。因此可以总结为下列判别条件。

判别条件一 H是群G的一个非空子集。H是G的子群的充分必要条件是：

1）如果$a,b\in H$，则$ab\in H$。

2）如果$a\in H$，则$a^{-1}\in H$。

证明 条件的必要性是显然的。为了证明充分性，只要证明单位元素e属于H就行了。因为H是非空集合，可取$a\in H$。由2)，$a^{-1}\in H$。再由1)，$aa^{-1}=e\in H$。▎

这两个条件还可以综合成一条，这就是

判别条件二 群G的非空子集H是一个子群的充分必要条件是：如果$a,b\in H$，则$ab^{-1}\in H$。

证明 条件的必要性是显然的。现在来证条件的充分性。设G的非空子集H满足判别条件二。任取$a\in H$，则$aa^{-1}=e\in H$。由此又有$ea^{-1}=a^{-1}\in H$。对于H中任两个元素a,b，上面已证$b^{-1}\in H$。于是$a(b^{-1})^{-1}=ab\in H$。所以判别条件一成立，H是G的一个子群。▎

对于有限子群来说，有更简单的判别条件。

判别条件三 设H是群G的一个有限非空子集。则H是G的子群的充分必要条件是H对G的运算是封闭的，即：如果$a,b\in H$，则$ab\in H$。

证明 条件的必要性是显然的。为了证明充分性，根据判别条件一，只要证明对于任意$a\in H$，都有$a^{-1}\in H$。下面来证明这一点。

设a是H中任一元素。因为H对运算是封闭的，所以a的正方幂也都属于H。又因H是一个有限集合，所以一定有自然数l，m使得$a^l=a^m$并且$l>m+1$。于是$l-m-1$是正整数，$a^{l-m-1}=a^{-1}\in H$。由判别条件一，H是G的一个子群。▎

如果G是一个有限群，那么G的子集都是有限集，因此总可以应用判别条件三来判断G的非空子集是否是一个子群。

例7 在整数加法群$\boldsymbol{Z}$中任意取定一个整数n，由n的一切倍数组成的集合记作$n\boldsymbol{Z}$：

$$n\boldsymbol{Z}=\{kn\mid k=0,\pm1,\pm2,\cdots\}.$$

因为对于$n\boldsymbol{Z}$中任意两个元素mn及ln，都有

$$mn-ln=(m-l)n\in n\boldsymbol{Z}.$$

所以根据判断条件二，$n\boldsymbol{Z}$是$\boldsymbol{Z}$的一个子群。

当$n=0$时，$n\boldsymbol{Z}=\{0\}$是由一个零元素组成的单位子群（也可称为零子群）。当$n=\pm1$时，$n\boldsymbol{Z}=\boldsymbol{Z}$。对任意的$n$，都有$(-n)\boldsymbol{Z}=n\boldsymbol{Z}$。而当$n\neq\pm m$时，$n\boldsymbol{Z}\neq m\boldsymbol{Z}$。

例8 n级正交矩阵全体O_n对矩阵的乘法组成一个群。

证明 O_n是$M_n(R)$的一个非空子集。因为两个正交矩阵的乘积还是正交矩阵，正交矩阵的逆矩阵也是正交矩阵，

所以满足判别条件一，O_n是$M_n(R)$的一个子群。因此 O_n 对矩阵的乘法成为一个群。

例9 设 a 是群 G 中一个元素。用$\langle a\rangle$表示由 a 的一切方幂组成的集合，则$\langle a\rangle$是 G 的一个子群。

证明 任取$\langle a\rangle$中两个元素a^l,a^m，都有

$$a^l(a^m)^{-1}=a^{l-m}\in\langle a\rangle.$$

故由判别条件二，$\langle a\rangle$是 G 的一个子群。

$\langle a\rangle$称为G**的由 a 生成的循环子群**，a 叫做它的**生成元**。$\langle a\rangle$的阶等于 a 的阶。

一般地，由一个元素生成的群称做**循环群**。关于这一类群，我们将在下一节中仔细讨论。

例10 G 是一个 n 元置换群，用G^+表示 G 中全部偶置换所成的集合。则G^+是 G 的一个子群。

证明 因为恒等置换是偶置换，所以G^+是 G 的有限非空子集。G^+中的元素都是 G 中偶置换，因此它们的乘积仍是 G 中偶置换，也属于G^+。故由判别条件三，G^+是 G 的子群。

例11 G 是一个群，用$Z(G)$表示 G 中与所有元素都可交换的元素全体：

$$Z(G)=\{a\,|\,ax=xa,\quad \forall\, x\in G\}.$$

请读者自己证明$Z(G)$是 G 的一个子群。

$Z(G)$ 称为G**的中心**。$Z(G)$中的元素称为 G **的中心元素**。如果G的中心是单位子群，那么G称为**无中心的**。G是交换群的充分必要条件是$Z(G)=G$。

例12 设H_1,H_2是群G的两个子群。由H_1 与 H_2 的公共元素组成的集合$H_1\cap H_2$称为H_1**与**H_2 **的交**：

$$H_1\cap H_2=\{a\,|\,a\in H_1,a\in H_2\}.$$

$H_1\cap H_2$也是 G 的子群。

证明 因为 $e\in H_1\cap H_2$，所以 $H_1\cap H_2$ 是 G 的一个非空子集。任取 $a,b\in H_1\cap H_2$。则$a,b\in H_1$；$a,b\in H_2$。因为H_1,H_2都是 G 的子群，所以 $ab^{-1}\in H_1$；$ab^{-1}\in H_2$。因此$ab^{-1}\in H_1\cap H_2$。由判断条件二，$H_1\cap H_2$是 G 的一个子群。

§4 循 环 群

4.1 循环群的定义及生成元

定义6 如果群G的每个元素都能表成一个固定元素a的方幂，那么G称为由 a 生成的**循环群**，记作$\langle a\rangle$。a 称为$\langle a\rangle$的一个**生成元**。

根据元素的阶的性质，可知循环群共有两种类型：

1 当生成元 a 是无限阶元素时，$\langle a\rangle$是一个无限阶循环群：

$$\langle a\rangle=\{\cdots,a^{-3},a^{-2},a^{-1},e,a,a^2,a^3,\cdots\}.$$

2 当生成元 a 是有限阶元素时，如果 a 的阶为 n，那么这时，

$$\langle a\rangle=\{e,a,a^2,\cdots,a^{n-1}\}$$

是一个 n 阶有限群。

例1 $\mathbf{Z}$是由 1 生成的无限循环群。$n\mathbf{Z}$ 是由 n 生成的无限循环群。

例2 n 个 n 次单位根对数的乘法组成一个 n 阶群 U_n。设 ε 是一个 n 次本原单位根，那么任一个 n 次单位根都可表成ε的一个方幂，因此U_n是一个循环群，ε 是它的一个生成元。

循环群的生成元不是唯一的。例如，$\mathbf{Z}$也可看成是由-1生成的循环群。在例 2 中ε 的取法也不是唯一的。那么，在

一个循环群中，怎样的元素才能作为生成元呢？为了解决这个问题，首先必须弄清楚生成元的条件。

设$\langle a\rangle$是由a生成的循环群，如果a^l是$\langle a\rangle$的一个生成元，那么$\langle a\rangle$中每个元素都可表成a^l的方幂。特别地，a也可以表成a^l的方幂。设

$$a=(a^l)^m=a^{lm}.$$

如果$\langle a\rangle$是无限循环群。那么a是无限阶元素。所以必须有

$$lm=1.$$

因此得出

$$l=\pm 1.$$

当然，容易看出，a及a^{-1}都是$\langle a\rangle$的生成元。

如果$\langle a\rangle$是一个n阶有限群，那么

$$n\,|\,lm-1.$$

因此

$$lm-1=nq,\quad lm-nq=1.$$

这说明l必须与n互素。另一方面，如果l与n互素，那么可找到整数u,v使

$$un+vl=1.$$

于是

$$(a^l)^v=a^{1-un}=a.$$

所以a可表成a^l的方幂。因而$\langle a\rangle$中任一元素也都可表成a^l的方幂，a^l是$\langle a\rangle$的一个生成元。

于是我们得到下面这个定理

定理6 1）无限循环群$\langle a\rangle$一共有两个生成元：a及a^{-1}。

2）n阶循环群$\langle a\rangle$中，元素a^l是$\langle a\rangle$的生成元的充要条件是$(n,l)=1$。所以$\langle a\rangle$一共有$\varphi(n)$个生成元($\varphi(n)$是欧拉函数)。

例3 设ε是一个12次本原单位根。则全部12次单位根所成的群U_{12}是由ε生成的循环群：

$$U_{12}=\langle\varepsilon\rangle=\{\varepsilon^k\,|\,k=0,1,2,\cdots,11\}.$$

U_{12}一共有$\varphi(12)=4$个生成元：

$$\varepsilon,\varepsilon^5,\varepsilon^7,\varepsilon^{11}.$$

4.2 循环群的子群

在循环群$\langle a\rangle$中任取一个元素a^k，可以生成一个循环群$\langle a^k\rangle$。我们来证明$\langle a\rangle$的每个子群都可以这样生成，即循环群的子群都是循环群。

定理7 1）无限循环群的非单位子群都是无限循环群。

2）n阶有限循环群$\langle a\rangle$的子群都是循环群，其阶为n的因子，而且对于n的每个因子d都有唯一的一个子群以d为阶。因此$\langle a\rangle$的子群的个数等于n的正因子的个数。

证明 首先来证明循环群的子群都是循环群。

设H是循环群$\langle a\rangle$的一个子群。如果H是单位子群，那么H当然是循环群。如果H不是单位子群，那么H中一定有a的正方幂，设a^m是H中指数最小的正方幂，来证$H=\langle a^m\rangle$。任取H中一个元素a^l。存在整数q及r，满足

$$l=qm+r,\quad 0\leqslant r<m.$$

于是

$$a^l(a^{-m})^q=a^r\in H.$$

由m的取法知必有$r=0$。于是$a^l=(a^m)^q\in H$。所以

$$H=\langle a^m\rangle.$$

因为无限循环群中的非单位元素都是无限阶元素，所以无限阶循环群的子群也都是无限循环群。

如果$\langle a\rangle$是 n 阶有限群，则由上面的证明可知m能整除n。因此a^m的阶是 n 的因子n/m。$\langle a^m\rangle$的阶也等于 n/m。

对于 n 的任一个因子 d，$\langle a^{n/d}\rangle$ 就是$\langle a\rangle$的一个 d 阶子群，并且从上面的证明知道$\langle a\rangle$的 d 阶子群可以由$\langle a\rangle$中的 d 阶元素$a^{n/d}$生成，所以是唯一的。▎

例4 因为12一共有 6 个正因子：1,2,3,4,6,12。所以U_{12}共有 6 个子群：

1 阶子群 $H_1=\langle\varepsilon^{12}\rangle=e$。

2 阶子群 $H_2=\langle\varepsilon^6\rangle=\{e,\varepsilon^6\}$。

3 阶子群 $H_3=\langle\varepsilon^4\rangle=\{e,\varepsilon^4,\varepsilon^8\}$。

4 阶子群 $H_4=\langle\varepsilon^3\rangle=\{e,\varepsilon^3,\varepsilon^6,\varepsilon^9\}$。

6 阶子群 $H_5=\langle\varepsilon^2\rangle=\{e,\varepsilon^2,\varepsilon^4,\varepsilon^6,\varepsilon^8,\varepsilon^{10}\}$。

12阶子群 $H_6=\langle\varepsilon\rangle=U_{12}$。

§5 陪集 群的陪集分解

设H是群G的一个子群。在有些问题中，为了讨论G与H的关系，并且应用H来讨论G，常常需要将G按照子群H分解成一些没有公共元素的子集的并。

例如，在整数加群$\boldsymbol{Z}$中，所有 7 的倍数组成一个子群$7\boldsymbol{Z}$。其余的数可以按照用 7 来除所得的余数分类，余数相同的数组成一类。把余数为 i 的类记作$i+7\boldsymbol{Z}$：

$$i+7\boldsymbol{Z}=\{i,i\pm7,i\pm14,i\pm21,\cdots\},\quad i=1,2,\cdots,6.$$

而$\boldsymbol{Z}$可以表成$7\boldsymbol{Z}$与这些类的并：

$$\boldsymbol{Z}=7\boldsymbol{Z}\cup(1+7\boldsymbol{Z})\cup(2+7\boldsymbol{Z})\cup\cdots\cup(6+7\boldsymbol{Z}).$$

现在考虑一般的情形。

定义7 设H是群G的一个子群，a是G中一个元素，用 a 右乘H中一切元素所得的集合记作Ha：

$$Ha=\{xa\mid x\in H\}.$$

称为H在G中的一个**右陪集**。同样可以定义H在G中的**左陪集**aH：

$$aH=\{ax\mid x\in H\}.$$

以下对右陪集进行讨论。关于右陪集的结果对于左陪集也成立。

子群H在G中的右陪集有下述一些性质：

1）Ha中元素个数与H一样。

这是因为由$xa=ya$可推出$x=y$。

2）H本身也是H的一个右陪集：$H=He$。$Ha=H$的充分必要条件是$a\in H$。

3）a在陪集Ha中。

根据这一点，我们把 a 叫做右陪集Ha的一个**陪集代表**。

4）对于右陪集中任一个元素 b，都有$Ha=Hb$。

证明 因为$b\in Ha$，所以有$h\in H$使$b=ha$。于是

$$Hb=Hha=Ha.\ ▎$$

这一点说明右陪集 Ha 中任一个元素都可以取作陪集代表。从这一点还可推出：

5）$Ha=Hb\Longleftrightarrow ab^{-1}\in H$。

6）任意两个右陪集Ha及Hb或者相等或者不相交。即

$$Ha=Hb\ \text{或}\ Ha\cap Hb=\varnothing.$$

证明 如果$Ha\cap Hb\neq\varnothing$，则它们包含公共元素 c：

$$c\in Ha,\quad c\in Hb.$$

因此，由4)得

$$Ha=Hc,\quad Hb=Hc.$$

因而有 $Ha=Hb$。 ▌

由于每个元素 a 都属于一个右陪集Ha，故可将有限群G对于子群分解成一些互不相交的右陪集的并：

$$G=Ha_1\cup Ha_2\cup\cdots\cup Ha_r,\quad Ha_i\cap Ha_j=\varnothing,$$
$$i,j=1,2,\cdots,r;\quad i\neq j.$$

这个式子称为G对H的**（右）陪集分解式**。其中 r 是右陪集的个数，称为H在G中的**指数**，记作$|G:H|$。$a_1,a_2,\cdots,a_r$称为H在G中的一个**右陪集代表系**。

类似地，群G也可以表成子群H的互不相交的左陪集的并，称为G对H的左陪集分解式。也可定义H在G中的左陪集代表系。显然，H在G中的右陪集个数与左陪集个数是相等的，都等于H在G中的指数。

从一个群对子群的陪集分解式可以得到下述关于子群的阶的重要定理。

定理8（Lagrange 定理） 群G的阶等于子群H的阶及H在G中的指数的乘积：

$$|G|=|H|\cdot|G:H|.$$

证明 设G对H的陪集分解式为：

$$G=Ha_1\cup Ha_2\cup\cdots\cup Ha_r.$$

因为$|Ha_i|=|H|$，$i=1,2,\cdots,r$。所以

$$|G|=|H|\cdot r=|H|\cdot|G:H|.$$ ▌

推论 有限群G中每个元素的阶都是G的阶$|G|$的因子。如果G的阶等于n，那么G中每个元素都满足方程

$$x^n=e.$$

证明 设a是G中一个m阶元素。则$H=\langle a\rangle$是G的一个m阶子群。根据上述定理，即得$m\,|\,|G|$。根据元素的阶的性质，即得另一个结论。 ▌

例1 n元交错群A_n在n元对称群S_n中的指数为2：

$$S_n=A_n\cup A_n(1,2).$$

例2 考虑上节例4中的群U_{12}及其4阶子群H_4：

$$U_{12}=H_4\cup H_4\varepsilon\cup H_4\varepsilon^2.$$

所以$|U_{12}:H_4|=3$。

例3 用G_1表示$G=S_n$中保持1不动的全部置换。如果$\sigma,\tau\in G_1$，则$1^\sigma=1^\tau=1$。因此$1^{\sigma\tau}=(1^\sigma)^\tau=1$，$\sigma\tau\in G_1$。所以$G_1$是$G$的一个子群。

下面来证明$e,(1,2),(1,3),\cdots,(1,n)$组成$G_1$在$G$中的一个右陪集代表系。

首先，这n个元素属于G_1的不同右陪集，这是因为

$$e(1,i)^{-1}=(1,i)\notin G,\quad i=2,3,\cdots,n;$$
$$(1,j)(1,i)^{-1}=(1,j,i)\notin G,\quad i,j=2,3,\cdots,n;\quad i\neq j.$$

所以陪集

$$G_1=Ge,G_1(1,2),\cdots,G_1(1,n)$$

两两不同。

其次，可证G中任一元素都属于上列陪集中的一个。对任一$\sigma\in G$。如果$1^\sigma=1$，则$\sigma\in G$。如果$1^\sigma=i\neq1$。则

$$1^{\sigma(1,i)^{-1}}=1^{\sigma(1,i)}=1.$$

所以 $\sigma\in G_1(1,i)$。

因此，$G=S_n$对G_1的右陪集分解为：

$$S_n=G_1\cup G_1(1,2)\cup G_1(1,3)\cup\cdots\cup G_1(1,n).$$

$e,(1,2),(1,3),\cdots,(1,n)$是$G_1$在$S_n$中的一个右陪集代表系。$G_1$在$S_n$中的指数为$n$。

例4 设G是一个置换群，仍用G^+表示G中全部偶置换组成的子群。如果G中没有奇置换，那么$G=G^+$。如果G中有奇置换，那么对于G中任意两个奇置换σ,τ，$\sigma\tau^{-1}$是G中

一个偶置换，因此$\sigma\tau^{-1}\in G^+$。这说明G中的奇置换都属于G^+的同一个陪集。任取G中一个奇置换σ，就可得到G对G^+的陪集分解

$$G=G^+\cup G^+\sigma.$$

总结以上分析，得

$$|G:G^+|=\begin{cases}1, & \text{如果}G\text{中无奇置换；}\\ 2, & \text{如果}G\text{中有奇置换。}\end{cases}$$

这是关于置换群的一个重要性质，今后常常要用到。

最后，我们来证明关于子群的指数及陪集分解的一个重要性质。

定理9 设

$$G\geqslant H\geqslant K.$$

则

1）$|G:K|=|G:H|\cdot|H:K|$。

2）如果G对H的陪集分解为：

$$G=Hg_1\cup Hg_2\cup\cdots\cup Hg_l,\qquad Hg_1=H;$$

H对K的陪集分解为：

$$H=Kh_1\cup Kh_2\cup\cdots\cup Kh_m,\qquad Kh_1=K,$$

则G对K的陪集分解为：

$$G=\bigcup_{\substack{i=1,\cdots,m\\ j=1,\cdots,l}}Kh_ig_j,\qquad Kh_1g_1=K.$$

3）如果G对K的陪集分解为：

$$G=Ka_1\cup Ka_2\cup\cdots\cup Ka_t,\qquad Ka_1=K.$$

那么可以适当地排列a_i的次序，使得

$$H=Ha_1=Ka_1\cup Ka_2\cup\cdots\cup Ka_m,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$Ha_{m+1}=Ka_{m+1}\cup Ka_{m+2}\cup\cdots\cup Ka_{2m},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$Ha_{(l-1)m+1}=Ka_{(l-1)m+1}\cup Ka_{(l-1)m+2}\cup\cdots\cup Ka_{lm},\quad (lm=t).$$

而且G对H的陪集分解为：

$$G=Ka_1\cup Ka_{m+1}\cup\cdots\cup Ka_{(l-1)m+1}.$$

证明 1）因为$|G|=|G:H|\cdot|H|$,

$$|H|=|H:K|\cdot|K|,$$

所以

$$|G|=|G:H|\cdot|H:K|\cdot|K|,$$

即

$$|G:K|=|G:H|\cdot|H:K|.$$

2）陪集Kh_ig_j（$i=1,2,\cdots m$；$j=1,2,\cdots,l$）共有lm个。与G对K的指数相等。因此只要证明这些陪集两两不相交就可以了。如果

$$Kh_ig_j=Kh_{i'}g_{j'},\quad 1\leqslant i,i'\leqslant m,\quad 1\leqslant j,j'\leqslant l.$$

则

$$h_ig_j(h_{i'}g_{j'})^{-1}=h_ig_jg_{j'}^{-1}h_{i'}^{-1}\in K\leqslant H.$$

因为$h_i,h_{i'}\in H$，所以

$$g_jg_{j'}^{-1}\in H.$$

这说明

$$Hg_j=Hg_{j'}.$$

于是$g_j=g_{j'}$，$j=j'$。从而

$$h_ih_{i'}^{-1}\in K.$$

同样的理由可得$h_i=h_{i'}$，$i=i'$。因此这lm个陪集是两两不相交的。

3）因为K在H中的陪集也一定是K在G中的陪集，因

此一定是 Ka_i $(i=1,2,\cdots,t)$ 中的一部分。可以调动 次序使

$$H=Ka_1\cup Ka_2\cup\cdots\cup Ka_m\quad(m=|K:H|).$$

于是 $a_{m+1}\overline{\in}H$，考虑H的陪集

$$Ha_{m+1}=Ka_1a_{m+1}\cup Ka_2a_{m+1}\cup\cdots\cup Ka_ma_{m+1},$$

陪集 $Ka_1a_{m+1},Ka_2a_{m+1},\cdots,Ka_ma_{m+1}$各不相同，而且与$Ka_1$，$Ka_2,\cdots,Ka_m$也都不同。因此可以调动 a_i的次序使

$$Ha_{m+1}=Ka_{m+1}\cup Ka_{m+2}\cup\cdots\cup Ka_{2m}.$$

这样逐次调动即可得到最后的分解式。▎

推论 设$G\geqslant H\geqslant K$。则

1）如果 $g_1,g_2,\cdots,g_l$是H在G中的一个右陪集代表系，$h_1,h_2,\cdots,h_m$是K在H中的一个右陪集代表系，那么

$$g_1h_1,g_1h_2,\cdots,g_1h_m,g_2h_1,g_2h_2,\cdots,$$
$$g_2h_m,\cdots,g_lh_1,g_lh_2,\cdots,g_lh_m$$

是K在H中的一个右陪集代表系。特别地，如果取 $g_1=e$，那么这个右陪集代表系中包含H对K的陪集代表系 $h_1,h_2,\cdots,h_m$。

2）在G对K的任一个右陪集代表系中，总能找出一部分组成H对K的右陪集代表系。

§6 同 构

设G和G_1是两个群，在很多情况下往往会提出这样的问题：G和G_1是否有相同的构造？什么叫做构造相同呢？要回答这个问题，必须建立同构的概念。

定义8 设G和G_1是两个群。如果存在一个由G到G_1上的一一映射φ，对于G中任意两个元素a，b，都有

$$(ab)^\varphi=a^\varphi b^\varphi.$$

那么就称 **G 同构于 G_1**，记作$G\cong G_1$。φ称为G到G_1的一个**同构映射**(简称**同构**)。当$G=G_1$时，φ称为G的一个**自同构映射**(简称**自同构**)。

例1 n维实向量空间$\boldsymbol{R}^n$的可逆线性变换群$L_n(R)$与n级可逆实矩阵群$M_n(R)$是同构的。

证明 在$\boldsymbol{R}^n$中取定一组基$\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n$。$\boldsymbol{R}^n$的每个线性变换$\boldsymbol{A}$在这组基下对应于一个实矩阵，而且当且仅当$\boldsymbol{A}$为可逆线性变换时，$A$为可逆矩阵。由于不同的线性变换在同一组基下的矩阵是不同的，映射

$$\varphi:\ \boldsymbol{A}\mapsto A$$

是$L_n(R)$到$M_n(R)$上的一个一一映射。我们知道，映射φ保持乘法，所以φ是$L_n(R)$到$M_n(R)$的一个同构映射。故有$L_n(R)\cong M_n(R)$。

例2 §1例8中的群G与置换群

$$K=\{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$$

是同构的。

证明 G到K的映射φ：

$$a\mapsto e,\quad b\mapsto(1,2)(3,4),$$
$$c\mapsto(1,3)(2,4),\quad d\mapsto(1,4)(2,3)$$

是一个一一映射而且保持运算，所以是一个同构映射，因而$G\cong K$。

读者可以再找一个G到K的同构映射。

例3 $S_3=\{e,(1,2),(1,3),(2,3),(1,2,3),(1,3,2)\}$。定义$S_3$到自身的一个映射：

$$e\mapsto e,\quad (1,2)\mapsto(2,3),\quad (1,3)\mapsto(1,2),$$
$$(2,3)\mapsto(1,3),\quad (1,2,3)\mapsto(1,2,3),\quad (1,3,2)\mapsto(1,3.2)$$

请读者验证这个映射是S_3的一个自同构映射。

群的同构关系是一个等价关系。也就是说，群的同构映射具有下列三条性质：

1）反身性：$G\cong G$。

2）对称性：如果$G\cong G_1$，则有$G_1\cong G$。

3）传递性：如果$G\cong G_1$，$G_1\cong G_2$，则有$G\cong G_2$。

这是因为恒等映射，同构映射的逆映射以及两个同构映射的乘积都是同构映射的缘故。

因为群的同构映射是一个一一映射，所以同构的群有相同的阶。下面来证明群的同构映射的一些重要性质。

设φ是群G到G_1的一个同构映射，则有

1）φ将G的单位元素e映到G_1的单位元素e_1。

证明 因为$e^2=e$，所以

$$(e^2)^\varphi=e^\varphi.$$

于是

$$e^\varphi e^\varphi=e^\varphi=e^\varphi e_1.$$

根据消去律，即得

$$e^\varphi=e_1. \quad \blacksquare$$

2）φ将G中元素a的逆元素a^{-1}映到a的象a^φ的逆元素$(a^\varphi)^{-1}$。即

$$(a^{-1})^\varphi=(a^\varphi)^{-1}.$$

证明 因为$aa^{-1}=e$，所以

$$(aa^{-1})^\varphi=e^\varphi, \quad a^\varphi\cdot(a^{-1})^\varphi=e_1.$$

因此

$$(a^{-1})^\varphi=(a^\varphi)^{-1}. \quad \blacksquare$$

3）G中元素a与它在G_1中的象a^φ有相同的阶。

证明 这是因为

$$a^k=e \rightleftarrows (a^\varphi)^k=e_1$$

的缘故。$\blacksquare$

4）对G中元素a,b有

$$ab=ba \rightleftarrows a^\varphi b^\varphi=b^\varphi a^\varphi.$$

证明 由定义即得。$\blacksquare$

设a,b是群中两个元素，如果$ab=ba$，就称这两个元素是可交换的。上述性质说明群的同构映射保持元素在运算下的交换性。由此可知，φ把G的中心元素映到G_1的中心元素，所以交换群的同构象也一定是交换群。

5）设H是G的一个子集。用H^φ表示H中元素在φ下的象组成的集合：

$$H^\varphi=\{h^\varphi \mid h\in H\}.$$

则H是G的子群当且仅当H^φ是G_1的子群。

证明 如果$H\leqslant G$，对G_1中任意两个元素a_1,b_1，因为φ是一一映射，故有$a,b\in H$使

$$a^\varphi=a_1, \quad b^\varphi=b_1.$$

于是$ab^{-1}\in H$，且

$$(ab^{-1})^\varphi=a^\varphi(b^{-1})^\varphi=a^\varphi(b^\varphi)^{-1}=a_1b_1^{-1}\in H^\varphi.$$

所以$H^\varphi\leqslant G_1$。

如果$H^\varphi\leqslant G_1$，则对G中任意两个元素a,b，都有

$$(ab^{-1})^\varphi=a^\varphi(b^{-1})^\varphi=a^\varphi(b^\varphi)^{-1}\in H^\varphi.$$

因为φ是一一映射，所以

$$ab^{-1}\in H.$$

因此$H\leqslant G$。$\blacksquare$

同构的定义及性质说明，在同构映射下，对应的元素在各自的运算之下有相同的关系。因此，如果我们抽象地研究一个群，也就是说如果不考虑群的元素是什么，也不考虑群中的运算是怎样定义的，而只考虑群在所定义的运算下的代

数性质，那么同构的群是可以不加区别的。例如，可以证明同阶的循环群一定是同构的，因此从同构的角度来看，对于任一个自然数 n，都恰有一个 n 阶循环群。

§7 群的置换表示

置换群是比较具体的一种群，它的元素和运算都可以具体地写出来。置换群之所以重要还在于：每个有限群都和一个置换群同构。我们知道同构的群具有相同的构造，说得具体一些，就是：有关群的那些不依赖于元素的特性而根据运算的性质就可以证明的结论，都能够自动地转移到与这个群同构的群上去。例如，两个同构的群有相同的阶，与一个交换群或循环群同构的群一定也是交换群或循环群，等等。因此，可以应用置换群来研究一般群。

这一节介绍将一个群表示成置换群的几种方法。

7.1 右正则表示

设 G 是一个群，阶等于 n。它的元素是

$$a_1=e, a_2, \cdots, a_n.$$

取定一个元素 a_i，用它依次右乘 G 中每个元素，得到 n 个元素

$$a_1a_i, a_2a_i, \cdots, a_na_i.$$

这 n 个元素仍在 G 中。而且由消去律可知这 n 个元素各不相同。因此它们是 $a_1, a_2, \cdots, a_n$ 的一个排列。作 $a_1, a_2, \cdots, a_n$ 的置换

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1a_i & a_2a_i & \cdots & a_na_i \end{pmatrix},$$

简记成 $\begin{pmatrix} a \\ aa_i \end{pmatrix}$。以后我们把这个置换记作 σ_{a_i}，简记作 σ_i。

用这个方法，我们得到 n 个 n 元置换 $\sigma_i(i=1,2,\cdots,n)$，其中单位元素 a_1 对应的置换是恒等置换。因为 σ_i 把单位元素 a_1 映到 $a_1a_i=a_i$，所以这 n 个置换各不相同。用 R_G 表示这 n 个置换所成的集合：

$$R_G=\{\sigma_1, \sigma_2, \cdots, \sigma_n\}.$$

这是作用于 $\{a_1, a_2, \cdots, a_n\}$ 上的 n 元对称群 S_n 的一个非空子集。下面来证明 R_G 是 S_n 的一个子群，并且 G 与 R_G 同构。

首先来证明

引理1 R_G 是 S_n 的一个子群。

证明 在 R_G 中任取两个置换 σ_{a_i} 与 σ_{a_j}。它们的乘积

$$\sigma_{a_i}\sigma_{a_j}=\begin{pmatrix} a \\ aa_i \end{pmatrix}\begin{pmatrix} a \\ aa_j \end{pmatrix}=\begin{pmatrix} a \\ aa_ia_j \end{pmatrix}$$
$$=\sigma_{a_ia_j}\in R_G.$$

所以根据子群的判别条件三，R_G 是 S_n 的一个子群。▌

其次来证明

引理2 G 与 R_G 是同构的。

证明 考虑 G 到 R_G 上的映射：

$$a_i \mapsto \sigma_{a_i},$$

来证这是一个同构映射。因为当 $a_i \neq a_j$ 时，$\sigma_{a_i} \neq \sigma_{a_j}$，所以这是一个一一映射。因此为了证明它是一个同构映射，只要证明它保持运算就可以了。而这一点在引理 1 中已经证明过了。▌

R_G 中的置换有一个特点：或者把每个元素都保持不变

(恒等置换就是这样)。或者没有不变元素(其它置换都这样)。这样的置换称做**正则置换**,而 R_G 称做 G 的**右正则表示**。

以上的讨论给出了构造与已知群同构的置换群的一个方法。从而证明了

定理9(Cayley) 每个 n 阶群都与一个 n 元(n 次)置换群同构。

下面来看儿个例子。

例1 G 是一个 6 阶循环群, a 是 G 的一个生成元:

$$G=\{e=a^0=a^6,a,a^2,a^3,a^4,a^5\}.$$

求 G 的右正则表示。

解 $e\mapsto\sigma_e$(恒等置换),

$$a\mapsto\sigma_a=\begin{pmatrix} e & a & a^2 & a^3 & a^4 & a^5 \\ a & a^2 & a^3 & a^4 & a^5 & e \end{pmatrix}.$$

因为置换的性质与它所作用的文字的符号没有关系,所以为了方便起见,可以写成:

$$\sigma_a=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}=(1,2,3,4,5,6).$$

σ_a 是一个 6 阶轮换。R_G 就是 σ_a 生成的 6 阶循环群:

$$R_G=\{\sigma_e=\sigma_a^6,\sigma_a,\sigma_a^2,\sigma_a^3,\sigma_a^4,\sigma_a^5\}.$$

例2 设 G 是由 a, b 两个元素生成的有限群。G 中元素的运算满足下述关系:

$$a^4=e,\qquad a^2=b^2\neq e,\qquad ab=ba^3.$$

从这些关系式可以推出 G 中共有 8 个元素:

$$G=\{e,a,a^2,a^3,b,ab,a^2b,a^3b\}.$$

而 G 的乘法表是:

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2
b	b	a^3b	a^2b	ab	a^2	a	e	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	e
a^2b	a^2b	ab	b	a^3b	e	a^3	a^2	a
a^3b	a^3b	a^2b	ab	b	a	e	a^3	a^2

这个群叫做**四元数群**。下面来求它的右正则表示。

$e\mapsto\sigma_e$(恒等置换),

$$a\mapsto\sigma_a=\begin{pmatrix} e & a & a^2 & a^3 & b & ab & a^2b & a^3b \\ a & a^2 & a^3 & e & a^3b & b & ab & a^2b \end{pmatrix}.$$

因为置换的作用与文字的符号无关,所以为了简便起见,我们把 G 中元素编号

$$e\mapsto1,\quad a\mapsto2,\quad a^2\mapsto3,\quad a^3\mapsto4,$$
$$b\mapsto5,\quad ab\mapsto6,\quad a^2b\mapsto7,\quad a^3b\mapsto8.$$

于是 σ 可写成

$$\sigma_a=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 8 & 5 & 6 & 7 \end{pmatrix}$$

$$=(1,2,3,4)(5,8,7,6).$$

同样可以算出:

$$\sigma_{a^2}=\begin{pmatrix} e & a & a^2 & a^3 & b & ab & a^2b & a^3b \\ a^2 & a^3 & e & a & a^2b & a^3b & b & ab \end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6&7&8\\3&4&1&2&7&8&5&6\end{pmatrix}$$

$$=(1,3)(2,4)(5,7)(6,8).$$

$$\sigma_{a^3}=\begin{pmatrix}e&a&a^2&a^3&b&ab&a^2b&a^3b\\a^3&e&a&a^2&ab&a^2b&a^3b&b\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6&7&8\\4&1&2&3&6&7&8&5\end{pmatrix}$$

$$=(1,4,3,2)(5,6,7,8).$$

$$\sigma_b=\begin{pmatrix}e&a&a^2&a^3&b&ab&a^2b&a^3b\\b&ab&a^2b&a^3b&a^2&a^3&e&a\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6&7&8\\5&6&7&8&3&4&1&2\end{pmatrix}$$

$$=(1,5,3,7)(2,6,4,8).$$

$$\sigma_{ab}=\begin{pmatrix}e&a&a^2&a^3&b&ab&a^2b&a^3b\\ab&a^2b&a^3b&b&a&a^2&a^3&e\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6&7&8\\6&7&8&5&2&3&4&1\end{pmatrix}$$

$$=(1,6,3,8)(2,7,4,5).$$

$$\sigma_{a^2b}=\begin{pmatrix}e&a&a^2&a^3&b&ab&a^2b&a^3b\\a^2b&a^3b&b&ab&e&a&a^2&a^3\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6&7&8\\7&8&5&6&1&2&3&4\end{pmatrix}$$

$$=(1,7,3,5)(2,8,4,6).$$

$$\sigma_{a^3b}=\begin{pmatrix}e&a&a^2&a^3&b&ab&a^2b&a^3b\\a^3b&b&ab&a^2b&a^3&e&a&a^2\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6&7&8\\8&5&6&7&4&1&2&3\end{pmatrix}$$

$$=(1,8,3,6)(2,5,4,7).$$

$$R_G=\{\sigma_e,\sigma_a,\sigma_{a^2},\sigma_{a^3},\sigma_b,\sigma_{ab},\sigma_{a^2b},\sigma_{a^3b}\}\cong G.$$

这个方法也可以用来讨论无限群。一般地，一个集合A（有限或无限）到自身的一个映射称为A的一个**变换**。A到自身的一一映射称为A的一个**可逆变换(或一一变换)**。用$S(A)$表示A的全部可逆变换所成的集合。易证$S(A)$对映射的乘法构成一个群，称为**A的全变换群**。由A的一部分可逆变换组成的群称为A的一个**变换群**。显然，A的变换群就是A的全变换群的子群。可以和证明定理9同样地证明：任何一个群都与一个变换群同构，而且从证明的方法可以看出，这个变换群可以取作某一个作用于这个群的变换群。

7.2 左正则表示

仍用$a_1=e,a_2,\cdots,a_n$表示n阶G群中全部元素。取定G中一个元素a_i。用a_i^{-1}依次左乘$a_1,a_2,\cdots,a_n$。也得到G中n个不同的元素：

$$a_i^{-1}a_1,a_i^{-1}a_2,\cdots,a_i^{-1}a_n.$$

这n个元素也各不相同，组成$a_1,a_2,\cdots,a_n$的一个排列，和上一节相仿，我们可以作一个n元置换

$$\tau_{a_i}=\begin{pmatrix}a_1&a_2&\cdots&a_n\\a_i^{-1}a_1&a_i^{-1}a_2&\cdots&a_i^{-1}a_n\end{pmatrix}=\begin{pmatrix}a\\a_i^{-1}a\end{pmatrix}.$$

这样，我们又得到作用于$\{a_1,a_2,\cdots,a_n\}$的n个n元置换。

组成 S_n 的另一个子集 L_G:

$$L_G=\{\tau_{a_1},\tau_{a_2},\cdots,\tau_{a_n}\}.$$

因为

$$\tau_{a_i}\tau_{a_j}=\begin{pmatrix}a\\a_i^{-1}a\end{pmatrix}\cdot\begin{pmatrix}a\\a_j^{-1}a\end{pmatrix}$$

$$=\begin{pmatrix}a\\a_j^{-1}a_i^{-1}a\end{pmatrix}=\begin{pmatrix}a\\(a_ia_j)^{-1}a\end{pmatrix}$$

$$=\tau_{a_ia_j}.$$

所以可以和前面一样地证明 L_G 是 S_n 的一个子群，映射

$$a_i\mapsto\tau_{a_i}$$

是 G 到 L_G 的一个同构映射. G 与置换群 L_G 是同构的. L_G 中的置换也都是正则置换，L_G 称为 G 的**左正则表示**. 证明留给读者，下面只给出一个例子.

例 3 求四元数群的左正则表示.

解 τ_e 是恒等置换.

$$\tau_a=\begin{pmatrix}x\\a^{-1}x\end{pmatrix}=\begin{pmatrix}x\\a^3x\end{pmatrix}$$

$$=\begin{pmatrix}e&a&a^2&a^3&b&ab&a^2b&a^3b\\a^3&e&a&a^2&a^3b&b&ab&a^2b\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6&7&8\\4&1&2&3&8&5&6&7\end{pmatrix}$$

$$=(1,4,3,2)(5,8,7,6).$$

$$\tau_{a^2}=(\tau_a)^2=(1,3)(2,4)(5,7)(6,8).$$

$$\tau_{a^3}=(\tau_a)^3=(1,2,3,4)(5,6,7,8).$$

$$\tau_b=\begin{pmatrix}x\\b^{-1}x\end{pmatrix}=\begin{pmatrix}x\\a^2bx\end{pmatrix}$$

$$=\begin{pmatrix}e&a&a^2&a^3&b&ab&a^2b&a^3b\\a^2b&ab&b&a^3b&e&a^3&a^2&a\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6&7&8\\7&6&5&8&1&4&3&2\end{pmatrix}$$

$$=(1,7,3,5)(2,6,4,8).$$

$$\tau_{ab}=\tau_a\tau_b=(1,8,3,6)(2,7,4,5).$$

$$\tau_{a^2b}=\tau_{a^2}\tau_b=(1,5,3,7)(2,8,4,6).$$

$$\tau_{a^3b}=\tau_{a^3}\tau_b=(1,6,3,8)(2,5,4,7).$$

$$L_G=\{\tau_e,\tau_a,\tau_{a^2},\tau_{a^3},\tau_b,\tau_{ab},\tau_{a^2b},\tau_{a^3b}\}\cong G.$$

读者学习到这里，也许会提出一个问题：为什么不用 a_i 来左乘 G 中各个元素，而要用 a_i^{-1} 来左乘呢？这个问题是值得考虑的. 如果用 a_i 来左乘，将 a_i 对应于置换

$$\tau'_{a_i}=\begin{pmatrix}a_1&a_2&\cdots&a_n\\a_ia_1&a_ia_2&\cdots&a_ia_n\end{pmatrix}.$$

这样也得到 n 个 n 元置换. 问题是，这 n 个置换是否也具有上面所说的那些性质呢？其实，由于 $\tau'_{a_i}=\tau_{a_i^{-1}}$，所以这样得到的 n 个置换所成的集合仍是 L_G. 但是，由于

$$\tau'_{a_i}\tau'_{a_j}=\begin{pmatrix}a\\a_ia\end{pmatrix}\begin{pmatrix}a\\a_ja\end{pmatrix}=\begin{pmatrix}a\\a_ja_ia\end{pmatrix}$$

$$=\begin{pmatrix}a\\(a_ja_i)a\end{pmatrix}=\tau'_{a_ja_i}.$$

因此，如果 G 是一个非交换群，那么映射

$$a_i\mapsto\tau'_{a_i}$$

就不是一个同构映射了。

7.3 陪集置换表示

上面介绍了群的正则表示，给出了与 n 阶群 G 同构的两个 n 元置换群。但是当 G 的阶比较大的时候，这两个置换群作用的文字比较多，运算也就比较复杂。因此为了减少置换所作用的文字个数，有时需要用其它方法将一个群表示为置换群。这一小节介绍用子群的陪集将群表成置换群的方法。

设 G 是一个群，H 是 G 的一个子群，G 的阶等于 n，H 在 G 中的指数等于 r。我们知道，G 可以分解成 H 的不相交的右陪集之并：

$$G=Hx_1\cup Hx_2\cup\cdots\cup Hx_r,$$

其中 $Hx_1=H$。

如果 a 是 G 中一个元素，那么用 a 右乘右陪集 Hx_i(即：用 a 右乘 Hx_i 中各个元素）得到一个右陪集 Hx_ia。用 a 依次右乘 H 的 r 个右陪集 Hx_i $(i=1,2,\cdots,r)$,得到 r 个右陪集

$$Hx_1a,Hx_2a,\cdots,Hx_ra.$$

这 r 个陪集各不相同，因此是原来 r 个陪集的一个排列。这样得到一个置换

$$\begin{pmatrix}Hx_1 & Hx_2 & \cdots & Hx_r\\ Hx_1a & Hx_2a & \cdots & Hx_ra\end{pmatrix}=\begin{pmatrix}Hx_i\\ Hx_ia\end{pmatrix}.$$

记作 ω_a。很明显地，单位元素 e 所对应的置换 ω_a 是恒等置换，而且

$$\omega_a\omega_b=\omega_{ab},\qquad \omega_{a^{-1}}=(\omega_a)^{-1}.$$

用 $S_{G/H}$ 表示由 $\omega_a(a\in G)$所成的集合

$$S_{G/H}=\{\omega_a|a\in G\}.$$

可以和以前一样证明 $S_{G/H}$ 是作用于 $\{Hx_1,Hx_2,\cdots,Hx_r\}$ 上的 r 元对称群 S_r 的一个子群。而且映射：

$$a\mapsto\omega_a,\qquad a\in G$$

是 G 到 $S_{G/H}$ 上的一个满映射，这个映射保持运算。$S_{G/H}$ 称为 G 对子群 H 的陪集置换表示。

例 4 G 是由 x，y 两个元素生成的有限群，G 中运算满足下述关系：

$$x^3=y^2=e,\qquad xy=yx^2.$$

从这些关系式，可以推知 G 中共有 6 个元素：

$$G=\{e,x,x^2,y,xy,x^2y\}.$$

用 H 表示 G 的由 y 生成的子群：

$$H=\langle y\rangle=\{e,y\}.$$

G 对 H 的陪集分解是：

$$G=H\cup Hx\cup Hx^2,$$

其中

$$Hx=\{x,x^2y\},\qquad Hx^2=\{x^2,x^2y\}.$$

下面来计算 G 对 H 的陪集置换表示：

$e\mapsto\omega_e$(恒等置换),

$$x\mapsto\omega_x=\begin{pmatrix}H & Hx & Hx^2\\ Hx & Hx^2 & H\end{pmatrix}=(1,2,3),$$

$$x^2\mapsto\omega_{x^2}=(\omega_x)^2=(1,3,2),$$

$$y\mapsto\omega_y=\begin{pmatrix}H & Hx & Hx^2\\ H & Hx^2 & Hx\end{pmatrix}=(2,3),$$

$$xy\mapsto\omega_{xy}=\omega_x\omega_y=(1,3),$$

$$x^2y \mapsto \omega_{x^2y} = (\omega_x)^2(\omega_y) = (1,2).$$

所以

$$S_{G/H} \cong S_3 \ .$$

例 5 设 G 是四元数群，H 为 a^2生成的 2 阶循环子群:

$$H = \{e, a^2\}.$$

求 $S_{G/H}$。

解 G 对 H 的陪集分解为:

$$G = H \cup Ha \cup Hb \cup Hab,$$

其中

$$Ha = \{a, a^3\}, \ Hb = \{b, a^2b\}, \ Hab = \{ab, a^3b\}.$$

把这些陪集编号:

$$H \mapsto 1, \ Ha \mapsto 2, \ Hb \mapsto 3, \ Hab \mapsto 4.$$

于是

$$e \mapsto \omega_e = (1)\text{(恒等置换)},$$

$$a \mapsto \omega_a = \begin{pmatrix} H & Ha & Hb & Hab \\ Ha & H & Hab & Hb \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1,2)(3,4),$$

$$a^2 \mapsto \omega_{a^2} = (\omega_a)^2 = (1),$$

$$a^3 \mapsto \omega_{a^3} = (\omega_a)^3 = \omega_a,$$

$$b \mapsto \omega_b = \begin{pmatrix} H & Ha & Hb & Hab \\ Hb & Hab & H & Ha \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1,3)(2,4),$$

$$ab \mapsto \omega_{ab} = \omega_a\omega_b = (1,4)(2,3),$$

$$a^2b \mapsto \omega_{a^2b} = (\omega_a)^2\omega_b = \omega_b,$$

$$a^3b \mapsto \omega_{a^3b} = (\omega_a)^3\omega_b = \omega_a\omega_b = \omega_{ab}.$$

所以

$$S_{G/H} = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

是 S_3的一个 4 阶子群。

群 G 到置换群 $S_{G/H}$ 上的映射:

$$a \mapsto \omega_a$$

是保持运算的。如果这个映射还是一一的，那么就是一个同构映射，此时 G 与 r 元置换群 $S_{G/H}$ 是同构的。例如，例 4 中的陪集置换表示就给出了群 G 与 S_3的一个同构映射，从而知道 $G \cong S_3$。但是，一般地这个映射不一定是一个一一对应。例如，例 5 中那个映射就不是一一的，这时，这个映射就不是一个同构映射，G 与 $S_{G/H}$ 就不是同构的。但是，既然这个映射保持运算，那么它一定能反映这两个群之间的一些关系。关于这一类映射以及由子群H的陪集得出的置换群与原来的群同构的条件等问题，将在下一章中进行讨论。

习　　题

1. 设 $a_1, a_2, \cdots, a_r$ 是群 G 中任意 $r(r \geqslant 2)$ 个元素，求证:

$$(a_1a_2\cdots a_r)^{-1} = a_r^{-1}a_{r-1}^{-1}\cdots a_2^{-1}a_1^{-1}.$$

2. 证明: 如果群 G 中每个元素的平方都等于单位元素，那么 G 一定是一个交换群。

3. 设 a, b 是群 G 中两个元素，求证:

(1) $a, a^{-1}, a^{-1}ba$ 有相同的阶。

(2) ab 与 ba 有相同的阶。

4. 设 a 是群 G 中一个元素，a 的阶等于 n。求证：a^m 的阶等于 $n/(n,m)$，其中 (n,m) 是 n 与 m 的最大公因数。

5. 设 a，b 是群 G 中两个可交换的元素，它们的阶分别为 l，m。试证：如果 $\langle a\rangle\cap\langle b\rangle=\{e\}$。则 ab 的阶等于 l 与 m 的最小公倍数 $[l,m]$。

6. 试证：如果群 G 中只有一个 2 阶元素，那么这个元素一定是 G 的中心元素。

7. 证明 4 阶群都是交换的。

8. 设

$$\sigma=\begin{pmatrix}1&2&3&4&5&6\\5&6&3&1&4&2\end{pmatrix},$$

$$\tau=\begin{pmatrix}1&2&3&4&5&6\\3&4&6&2&5&1\end{pmatrix}$$

是 S_6 中两个置换。

(1) 写出 σ,τ 的轮换表法，并求 σ,τ 的阶。

(2) 计算 $\sigma\tau,\tau\sigma,\sigma^{-1},\sigma^2,\sigma^3,\tau^{-1}\sigma\tau$。

9. 解置换方程 $\sigma x=\tau$ 及 $y\sigma=\tau$，其中

$$\sigma=\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix},\quad \tau=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}.$$

10. 设 σ,τ 是两个 n 元置换，其中 σ 是一个 r-轮换：

$$\sigma=(a_1,a_2,\cdots,a_r).$$

试证：

$$\tau^{-1}\sigma\tau=(a_1^{\tau},a_2^{\tau},\cdots,a_r^{\tau})$$

并将这个结论推广到 σ 是一个任意置换的情形。

11. 证明 $S_n(n>2)$ 是无中心群。

12. 设 σ 的轮换表法为

$$\sigma=\sigma_1\sigma_2\cdots\sigma_s,$$

其中 $\sigma_i(i=1,2,\cdots,s)$ 的长度为 l_i。试证：σ 的奇偶与 $l_1+l_2+\cdots+l_s+s$ 一致。

13. 设 a 是群 G 中一个 n 阶元素，H 是 G 的一个子群。试证：如果 $a^m\in H,(n,m)=1$，则 $a\in H$。

14. 试证阶为素数的群一定是循环群。

15. 证明：群 G 没有非平凡子群的充分必要条件是 G 为素数阶循环群。

16. 设 G 是一个 pq 阶群，p,q 都是素数且 $p<q$。证明：G 不可能有两个不同的 q 阶子群。

17. A 是有限群 G 的一个非空子集。试证：当且仅当 $AA\subseteq A$ 时，A 是 G 的一个子群(群 G 的两个子集 A 与 B 的乘积 AB 定义为 $AB=\{ab\mid a\in A,b\in B\}$)。

18. 设 A，B 都是群 G 的子群。则当且仅当 $AB=BA$ 时，AB 是 G 的子群。

19. 设 A，B，C 都是 G 的子群。求证：如果 $A\leqslant C$，则 $AB\cap C=A(B\cap C)$。

20. 设 H 是群 G 的子群，$|G:H|=2$。证明：对于 G 中任一元素 a 都有 $Ha=aH$。

21. 求 S_4 对子群

$$K=\{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$$

的陪集分解。

22. 找出四元数群的全部子群及其陪集分解。

23. 试求 S_3 的左、右正则表示。

24. 求 S_4 对 S_3 的陪集置换表示并证明 S_4 与这个置换表示是同构的。

第二章　正规子群与同态定理

我们知道同构映射是一个一一映射并且保持运算，所以就保证了同构的群具有相同的构造。在有些问题中，我们还会遇到一些保持运算的映射，但是不一定是一一的。例如在上一节中我们利用子群的陪集分解所作的置换表示就是这样的。这种映射叫做同态映射。同态映射既然保持运算，它必然能反映这两个群之间的关系以及它们的一些共同的性质。由于一个群的同态象的阶比这个群的阶小，研究起来比较方便，找出一个群的同态象对于研究这个群是非常有用的。

这一章主要讨论同态映射的性质，以及一个群与其同态象的关系。

这一章还介绍一些重要的概念：共轭元素，共轭子群，正规子群，商群，特征子群，自同构群等。

正规子群等概念不仅在讨论同态映射时起着重要的作用，它们在整个群论中都占有很重要的地位。

§1　同　　态

定义 1　G与H是两个群，φ是G到H的一个映射。如果对于G中任意两个元素a，b，都有

$$(ab)^{\varphi}=a^{\varphi}b^{\varphi}.$$

φ就叫做G到H的一个**同态映射**。当φ是一个映上的同态时，φ称为一个**满同态**。H称为G的一个**同态象**。记作$G\sim H$。

要注意，$G\sim H$与$H\sim G$是不同的。

例 1　设H是G的一个子群，G到陪集置换表示$S_{G/H}$上的映射

$$a\mapsto\omega_a,\quad a\in G$$

是一个满同态映射，$S_{G/H}$是G的一个同态象。

例 2　设F是一个域，用$M_n(F)$表示系数在F中的全体n级可逆矩阵所成的乘法群。仍用F^*表示F中全体非零元素所成的乘法群。定义$M_n(F)$到F^*的映射φ为

$$A\mapsto A^{\varphi}=|A|,\quad A\in G.$$

$|A|$表示矩阵A的行列式。则因

$$(AB)^{\varphi}=|AB|=|A||B|=A^{\varphi}B^{\varphi},\quad A,B\in G,$$

所以φ是G到F^*的一个同态映射，而且，对于F^*中任一元素a，令

$$A(a)=\begin{pmatrix}a_1 & & \\ & \ddots & \\ & & 1\end{pmatrix}.$$

则$A(a)\in M_n(F)$，且

$$(A(a))^{\varphi}=|A(a)|=a.$$

所以φ是一个满同态，$M_n(F)\sim F^*$。

例 3　U_n是n次单位根所成的n阶循环群。取定一个n次本原单位根ε。定义整数加法群Z到U_n上的映射ψ：

$$k\mapsto k^{\psi}=\varepsilon^k,\qquad k\in Z.$$

ψ是一个满同态，$Z\sim U_n$。

同态映射有下述一些重要性质。

设φ是群G到H的一个同态映射。则有

1）φ将G的单位元素e映到H的单位元素e'。

2) φ 将 G 中元素 a 的逆元素 a^{-1}映到 a^{φ} 的逆元素:

$$(a^{-1})^{\varphi}=(a^{\varphi})^{-1}.$$

这两条性质可以与以前证明关于同构映射的相同性质一样证明，留给读者去完成.

3) a^{φ} 的阶是 a 的阶的一个因数.

证明 设 a 的阶为 k. 则 $a^{k}=e$. 于是

$$(a^{\varphi})^{k}=(a^{k})^{\varphi}=e^{\varphi}=e'.$$

所以 a^{φ} 的阶是 k 的一个因数. ▎

4) φ 把 G 中可交换的元素映到 H 中可交换的元素，即

$$ab=ba(a,b\in G)\to a^{\varphi}b^{\varphi}=b^{\varphi}a^{\varphi}.$$

如果 φ 是满同态，那么 φ 把 G 的中心元素映到 H 的中心元素.

需要注意的是，以 $a^{\varphi}b^{\varphi}=b^{\varphi}a^{\varphi}$ 不能推出 $ab=ba$. 因此，即使 φ 是一个满同态，也只有 $(Z(G))^{\varphi}\leqslant Z(H)$.

5) 如果 A 是 G 的一个子群，则 A^{φ} 是 H 的一个子群.

6) 设 B 是 H 的一个子群. 用 $B^{\varphi^{-1}}$ 表示 B 的逆象，即

$$B^{\varphi^{-1}}=\{a\in G\,|\,a^{\varphi}\in B\}.$$

则 $B^{\varphi^{-1}}$ 是 G 的一个子群.

证明 因为 B 是一个子群，所以 $B^{\varphi^{-1}}$ 当然是 G 的一个非空子集. 如果 a，b 都在 $B^{\varphi^{-1}}$ 中，那么

$$a^{\varphi},b^{\varphi}\in B.$$

于是

$$(ab^{-1})^{\varphi}=a^{\varphi}(b^{\varphi})^{-1}\in B.$$

因此

$$ab^{-1}\in B^{\varphi^{-1}}.$$

所以 $B^{\varphi^{-1}}$ 是 G 的一个子群. ▎

当 $B=\{e'\}$ 是 H 的单位子群时，它的逆象也是 G 的一个子群，称为 φ 的核.

定义 2 设 φ 是群 G 到 H 的一个同态映射，e' 是 H 的单位元素. e' 的逆象

$$K=\{a\in G\,|\,a^{\varphi}=e'\}$$

是 G 的一个子群，称为 φ 的核.

同构映射是一一的同态映射. 可以应用同态映射的核来判断一个同态映射是不是同构映射.

定理 1 设 φ 是群 G 到 H 上的一个满同态映射. 则 φ 是同构映射的充分必要条件是 φ 的核 $K=\{e\}$.

证明 条件显然是必要的. 现在来证明条件也是充分的. 假设 $K=\{e\}$，来证 φ 是一个一一映射. 如果 G 中两个元素 a，b 在 φ 下的象相同:

$$a^{\varphi}=b^{\varphi}.$$

那么

$$(ab^{-1})^{\varphi}=a^{\varphi}(b^{\varphi})^{-1}=e'.$$

因此

$$ab^{-1}\in K.$$

由 $K=\{e\}$，得

$$ab^{-1}=e.$$

所以φ是一个一一映射，因而φ是一个同构映射. ▎

从定理的证明还可以看出：如果φ是 G 到 H 的一个同态映射，K 是φ的核，那么从$a^{\varphi}=b^{\varphi}$ 可以推出

$$ab^{-1}\in K.$$

因此 a,b 属于K的同一个右陪集. 另一方面，当a,b属于K的同一个右陪集时，一定有

$$a=bx,$$

其中 $x\in K$. 于是有

$$a^{\varphi}=(bx)^{\varphi}=b^{\varphi}x^{\varphi}=b^{\varphi}.$$

这就是说，G中两个元素在φ下的象相同的充分必要条件是a,b属于核K的同一个陪集。

由此可见，如果φ是G到H上的一个同态映射，K是φ的核，那么G在φ下的象集合G^φ可以由K在G中的一个陪集代表系的象得到。这就给出了构造群的同态象的一个方法。问题是：是不是G的每个子群都可以作为某个同态的核？更进一步，如果K是G到H上的一个同态映射的核，那么，K与H有什么关系？这些问题将在第3、第4两节中解决。

§2 共轭子群与共轭元素

在解决有关同态的一些问题以前，作为准备，我们先来介绍共轭子群与共轭元素的概念。

2.1 共轭子群

在我们作群G对子群H的陪集置换表示的时候，映射

$$\varphi:\ a\mapsto\begin{pmatrix}Hx_i\\Hx_ia\end{pmatrix}$$

一般地只是一个同态映射而不一定是同构映射。那么，在什么情形下这个映射是同构映射呢？根据定理1，我们只要讨论什么时候这个映射的核，即恒等映射的原象只有单位元素就可以了。

我们首先来看G中什么样的元素在φ下的象是恒等置换。如果a^φ是恒等置换，即

$$a^\varphi=\omega_a=\begin{pmatrix}Hx_i\\Hx_ia\end{pmatrix}=\omega_e(\text{恒等置换}),$$

那么就有

$$Hx_i=Hx_ia,\quad i=1,2,\cdots,r.$$

于是 $$x_iax_i^{-1}\in H,\quad i=1,2,\cdots,r.$$

设 $$x_iax_i^{-1}=h_i,\quad i=1,2,\cdots,r.$$

则 $$a=x_i^{-1}h_ix_i\in x_i^{-1}Hx_i,\quad i=1,2,\cdots,r.$$

其中 $$x_i^{-1}Hx_i=\{x_i^{-1}hx_i\,|\,h\in H\},\quad i=1,2,\cdots,r.$$

很容易验证$x_i^{-1}Hx_i$（$1\leqslant i\leqslant r$）是G的一个子群。令

$$k=\bigcap_i x_i^{-1}Hx_i.$$

那么上面的讨论说明a^φ为恒等置换的必要条件是$a\in K$。这个条件也是$a^\varphi=\omega_e$的充分条件。因此K就是φ的核。当且仅当$K=\{e\}$时，φ是同构映射。

子群$x_i^{-1}Hx_i$称为H的**共轭子群**。这一小节首先讨论共轭子群的一些性质。然后再进一步讨论陪集置换表示。

定义3 设H_1及H_2是群G的两个子群。如果存在G中一个元素a使得

$$a^{-1}H_1a=H_2,$$

则称H_1与H_2是**共轭的**。

子群的共轭关系具有下面一些性质：

1）每个子群都与自己共轭。

这是因为$e^{-1}He=H$。

2）如果H_1与H_2共轭，那么H_2与H_1共轭。

这是因为从$a^{-1}H_1a=H_2$可推出$(a^{-1})^{-1}H_2a^{-1}=H_1$。

3）如果H_1与H_2共轭，H_2与H_3共轭，那么H_1与H_2共轭。

理由是：从$a^{-1}H_1a=H_2$，$b^{-1}H_2b=H_3$可推出

$$(ab)^{-1}H_1(ab)=H_3.$$

因此，子群的共轭关系是一个等价关系。G的子群可以分成一些互不相交的共轭子群的集合，称为**共轭子群类**。在

同一个类中的子群都是共轭的，而不同类中的子群互不共轭。同一个共轭子群类中的子群都有相同的阶及指数。

例1 $A_4=\{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3),$
$(1,2,3),(1,3,2),(1,2,4),(1,4,2),$
$(1,3,4),(1,4,3),(2,3,4),(2,4,3)\}$。

A_4的子群可以分成下列五个共轭子群类：

$\{e\}$；

$\{e,(1,2)(3,4)\}$，$\{e,(1,3)(2,4)\}$，$\{e,(1,4)(2,3)\}$；

$\{e,(1,2,3),(1,3,2)\}$，$\{e,(1,2,4),(1,4,2)\}$，
$\{e,(1,3,4),(1,4,3)\}$，$\{e,(2,3,4),(2,4,3)\}$；

$\{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$；

A_4。

设$H_1,H_2,\cdots,H_l$是某个共轭子群类中全部子群。对于G中任一元素a，$a^{-1}H_ia$ $(i=1,2,\cdots,l)$仍然是这l个子群中的一个，而且当$i\neq j$时，$a^{-1}H_ia\neq a^{-1}H_ja$。所以

$$a^{-1}H_1a,a^{-1}H_2a,\cdots,a^{-1}H_la$$

是这l个子群的一个排列。由此可作一个置换：

$$\begin{pmatrix} H_1 & H_2 & \cdots & H_l \\ a^{-1}H_1a & a^{-1}H_2a & \cdots & a^{-1}H_la \end{pmatrix}.$$

可以用这种方法得到G的一个置换表示。这里就不仔细讨论了。

2.2 正规化子

设H是G的一个子群。这一小节讨论H的共轭子群的个数以及如何找出G的全部共轭子群。

作G的子集

$$N_G(H)=\{x\mid x^{-1}Hx=H\}.$$

因为单位元素在$N_G(H)$中，所以$N_G(H)$是G的一个非空子集。如果$x,y\in N_G(H)$，那么

$$x^{-1}Hx=H,\quad y^{-1}Hy=H.$$

于是

$$(x^{-1})^{-1}Hx^{-1}=H,$$
$$(xy)^{-1}H(xy)=y^{-1}(x^{-1}Hx)y=y^{-1}Hy=H.$$

因此 $$x^{-1}\in N_G(H),\quad xy\in N_G(H).$$

所以$N_G(H)$是G的一个子群。$N_G(H)$称做H在G内的**正规化子**。显然有$H\leqslant N_G(H)$。

可以应用$N_G(H)$来计算H的共轭子群的个数。

定理2 H在G中的共轭子群的个数等于其正规化子$N_G(H)$在G中的指数。

证明 $N_G(H)$在G中的指数等于$N_G(H)$的右陪集的个数。因此只要证明：对于G中两个元素a及b，共轭子群$a^{-1}Ha$与$b^{-1}Hb$相等的充分必要条件是a,b属于H的同一个右陪集。

容易看出，$a^{-1}Ha=b^{-1}Hb$的充分必要条件为

$$ba^{-1}Hab^{-1}=H.$$

即 $$(ab^{-1})^{-1}Hab^{-1}=H.$$

亦即 $$ab^{-1}\in N_G(H).$$

而这一条件又等价于a，b属于$N_G(N)$的同一个右陪集。▎

定理2的证明还告诉我们：H的全部共轭子群可以由$N_G(H)$在G中的一个右陪集代表系给出。

例2 设$G=S_4$，$H=\{e,(1,2),(3,4),(1,2)(3,4)\}$。计算$H$在$G$中的共轭子群。

根据计算，可得

$$N_G(H)=\{e,(1,2),(3,4),(1,2)(3,4),(1,3)(2,4),$$
$$(1,4)(2,3),(1,3,2,4),(1,4,2,3)\}。$$

所以$|G:N_G(H)|=3$。H有3个共轭子群，这3个共轭子群可以由$N=N_G(H)$的右陪集代表给出。因为

$$G=N\cup N(1,3)\cup N(1,4),$$

所以H的三个共轭子群为

$$H,$$
$$(1,3)^{-1}H(1,3)=\{e,(1,4),(2,3),(1,4)(2,3)\},$$
$$(1,4)^{-1}H(1,4)=\{e,(1,3),(2,4),(1,3)(2,4)\}。$$

现在我们回过来讨论G对子群H的陪集置换表示。我们在以前已经分析过，映射

$$a\mapsto\omega_a=\begin{pmatrix}Hx_i\\Hx_ia\end{pmatrix}$$

是一个同构映射的充要条件是

$$\bigcap_i x_i^{-1}Hx_i=\{e\},$$

其中$x_1,x_2,\cdots,x_r$是H在G中的一个右陪集代表系。因为H的全部共轭子群可以由$N_G(H)$在G中的陪集代表得出，又因$N_G(H)\geqslant H$,所以$N_G(H)$在G中的陪集代表可以在$x_1,x_2,\cdots,x_r$中选取。这说明$x_1^{-1}Hx_1,x_2^{-1}Hx_2,\cdots,x_r^{-1}Hx_r$给出了$H$的全部共轭子群(可能有重复的)。因此，我们有下述定理。

定理3 设H是G的一个子群。G对H的陪集置换表示$S_{G/H}$与G同构的充要条件是

$$\bigcap_{x\in G}x^{-1}Hx=\{e\}。$$

我们来回顾一下以前的例子。

在第一章§7例4中，应用上面的方法，可以算出H一共有三个共轭子群：

$$H,$$
$$x^{-1}Hx=\{e,xy\},$$
$$(x^2)^{-1}Hx^2=\{e,x^2y\}。$$

这三个子群的交等于$\{e\}$。所以G与$S_{G/H}$是同构的。

在第一章§7例5中，H是一个2阶子群，与H共轭的子群一定也是2阶子群。但是G中只有一个2阶元素。所以G只有一个2阶子群，H的共轭子群只有H自己。由此知

$$\bigcap_{x\in G}x^{-1}Hx=H。$$

从而映射

$$a\mapsto\omega_a=\begin{pmatrix}Hx_i\\Hx_ia\end{pmatrix}$$

的核就是H。G与$S_{G/H}$不是同构的。

2.3 共轭元素，中心化子

前面我们讨论了共轭子群。H的共轭子群$x^{-1}Hx$由形如$x^{-1}hx(h\in H)$的元素组成。$x^{-1}hx$称为h的**共轭元素**。

定义4 a,b是群G中两个元素，如果G中有一个元素x使$x^{-1}ax=b$，则称a与b是**共轭的**。

显然，共轭元素有相同的阶。

和子群的共轭关系一样，元素的共轭关系也有下述三个性质：

1) 任一元素a都与自己共轭。

2) 如果a与b共轭，那么b与a也共轭。

3) 如果a与b共轭，b与c共轭，那么a与c共轭。

因此，元素的共轭关系是一个等价关系

这三条性质的证明方法与前面关于共轭子群的证明相仿，这里就不再重复了。

根据这三条性质，G中元素可以分成一些互不相交的共轭元素的集合，称为**共轭元素类**。在同一类中的元素互相共轭，而不同类中的元素彼此不共轭。

例3 A_4的12个元素分成下列4个共轭元素类：

$$C_1=\{e\},$$
$$C_2=\{(1,2,3),(1,3,4),(1,4,2),(2,4,3)\},$$
$$C_3=\{(1,3,2),(1,4,3),(1,2,4),(2,3,4)\},$$
$$C_4=\{(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}.$$
$$A_4=C_1\cup C_2\cup C_3\cup C_4,\quad C_i\cap C_j=\phi\quad(i\neq j).$$

设G共有s个共轭类，记作$C_1,C_2,\cdots,C_s$。再设C_i中包含n_i个元素($i=1,2,\cdots,s$)。那么因为

$$G=C_1\cup C_2\cup\cdots\cup C_s$$

而且当$i\neq j$时，C_i与C_j没有公共元素。所以

$$|G|=n_1+n_2+\cdots+n_s.$$

下面来讨论G的共轭元素类中元素的个数。

和处理共轭子群的情形相仿，设a是群G的一个元素。作G的子群

$$Z_G(a)=\{x\mid x^{-1}ax=a\}.$$

很容易验证$Z_G(a)$是G的一个子群。子群$Z_G(a)$称为a在G内的**中心化子**。和共轭子群的个数一样，我们有下述结果。

定理4 a是群G中一个元素。a在G中的共轭元素的个数等于a在G内的中心化子$Z_G(a)$在G中的指数。

证明 只要证明，对于G中两个元素x,y，共轭元素$x^{-1}ax$与$y^{-1}ay$相等的充要条件是x与y属于$Z_G(a)$的同一个右陪集。证明了这一点以后，就知道a的共轭元素的个数等于$Z_G(a)$的右陪集的个数，即等于$Z_G(a)$的指数。这就是定理所要证明的。

易见$x^{-1}ax=y^{-1}ay$的充要条件为

$$a=yx^{-1}axy^{-1}=(xy^{-1})^{-1}a(xy^{-1}).$$

即
$$xy^{-1}\in Z_G(a).$$

而这个条件又是x,y属于$Z_G(a)$的同一个右陪集的充分必要条件。▎

从这个定理可以得到下列推论

推论 1）共轭元素类C_i中元素的个数n_i是G的阶的一个因子。

2）共轭元素的中心化子具有相同的指数，因而有相同的阶。

不仅如此，还可证明共轭元素的中心化子是共轭的（习题3）。

和讨论共轭子群的情形相仿，可以应用共轭元素类中的元素来作出群的置换表示。

§3 正规子群

这一节讨论“怎样的子群可以作为同态的核”这个问题。

设G是一个群，φ是G到群G_1的一个同态映射。我们曾经证明过，φ的核

$$K=\{x\in G\mid x^{\varphi}=e_1\}\quad(e_1\text{是}G_1\text{的单位元素})$$

是G的一个子群，而且K的一个右陪集Ka中的每个元素在φ下的象都是a^{φ}，而不同右陪集中的元素的象一定不同。如果我们仔细回想一下这些结论的证明，可以看出：把右陪集换成左陪集，这些结论仍然成立。因此得到下述结论：

设φ是群G到G_1的一个同态映射，K是φ的核。则对G的

任意元素 a，左陪集aK及右陪集Ka中元素在同态映射 φ 下的象都是a^{φ}。

又因为其它陪集中元素的象都与a^{φ}不同，所以必须有

$$aK = Ka, \quad \forall a \in G.$$

我们把这样的群称做正规子群。

定义5 设H是G的一个子群。如果G对H的右陪集分解与右陪集分解一致，H就称为G的一个**正规子群**。

以后，如果 H 是G的一个正规子群，就记作 $H \trianglelefteq G$（或$G \trianglerighteq H$）。如果H是G的一个正规的真子群，就记作$H \triangleleft G$（或$G \triangleright H$）。

从定义立即可以看到：G的平凡子群$\{e\}$及G都是G的正规子群。还可看到：交换群的子群都是正规的。下面再来举几个例子。

例1 在四元数群G中，仍设子群 $H = \{e, a^2\}$。已知G对H的陪集分解是

$$G = H \cup Ha \cup Hb \cup Hab.$$

可以验证，

$$Ha = aH, \quad Hb = bH, \quad Hab = abH.$$

所以

$$H \triangleleft G.$$

例2 群G的中心Z是G的一个正规子群。

因为Z与G中每个元素都可交换，所以对G中任意元素x，都有

$$Zx = xZ.$$

因此Z是G的一个正规子群。

例3 在A_4中取子群$H = \{e, (1,2)(3,4)\}$。那么

$$H(1,2,3) = \{(1,2,3), (1,3,4)\},$$

$$(1,2,3)H = \{(1,2,3), (2,4,3)\} \neq H(1,2,3).$$

所以H不是G的正规子群。

从上面的例子可以看到的确有不是正规子群的子群存在。而直接从正规子群的定义来判断某个子群是否是正规子群有时比较麻烦，因此，讨论正规子群的一些判别条件是很有必要的。

判别条件一 指数等于 2 的子群一定是正规的。

证明 设H是G的一个指数为 2 的子群。那么H共有两个右陪集，也共有两个左陪集。取$x \in G$，但$x \notin H$，就有

$$G = H \cup Hx = H \cup xH, \quad Hx = xH.$$

因此，G对H的左、右陪集分解相同，故$H \triangleleft G$。▎

由此可知 n 元交错群是 n 元对称群的一个正规子群。这是下述例子的一个特殊情形。

例4 设G是一个置换群。以前已经证明过G中全部偶置换组成的子集G^+是G的一个子群。并且

$$|G:G^+| = \begin{cases} 1, & \text{如果} G \text{中无奇置换}; \\ 2, & \text{如果} G \text{中有奇置换}. \end{cases}$$

即$G^+ = G$或G^+在G中的指数为 2。所以$G^+ \trianglelefteq G$。

判别条件二 设H是G的一个子群。$H \trianglelefteq G$ 的一个充分必要条件是：对G中任一元素 a，都有 $a^{-1}Ha = H$，即H只有一个共轭子群，就是H自己。

因此，正规子群也称**自共轭子群**。

证明 因为 $a^{-1}Ha = H \rightleftharpoons aH = Ha$，故由定义即可知

$$H \trianglelefteq G \rightleftharpoons a^{-1}Ha = H, \quad \forall a \in H. ▎$$

例5 求A_4的全部正规子群。

解 在§2例1中，我们已经求出了A_4的全部共轭子群类。由判别条件二，知子群H是正规子群的充分必要条件是

包含H的共轭类中只有H一个子群。所以可知A_4共有三个正规子群：

$$\{e\},\{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\},A_4.$$

共中只有一个非平凡正规子群。

从判别条件二可以看出，如果H是G的一个正规子群，那么H也是任一中间群G_1（$G\geqslant G_1\geqslant H$）的正规子群。而且，即使$H$不是$G$的正规子群，$H$也可能是某个中间群的正规子群。子群$H$在$G$内的正规化子$N_G(H)$就以$H$为正规子群，这一点可以从判别条件2看出。因此当$N_G(H)=G$时，$H\trianglelefteq G$，可以证明这个条件也是充分的。即有

判别条件三　$H\trianglelefteq G\rightleftharpoons N_G(H)=G$。

证明　$H\trianglelefteq G\rightleftharpoons x^{-1}Hx=H,\quad\forall x\in G$

$$\rightleftharpoons N_G(H)=G. \quad ▌$$

这个条件也可以叙述为：

判别条件四　G的子群H是正规子群的一个充分必要条件是：对G中任一元素g及H中任一元素h，都有

$$g^{-1}hg\in H.$$

例6　设H是G的一个子群。用$Z_G(H)$表示G中与H的每个元素都可交换的元素全体：

$$Z_G(H)=\{x\in G\mid xh=hx,\quad\forall h\in H\}.$$

容易看出：

$$Z_G(H)=\bigcap_{h\in H}Z_G(h).$$

所以$Z_G(H)$是G的一个子群，称为H在G内的**中心化子**。显然，$Z_G(H)\leqslant N_G(H)$。可证$Z_G(H)$是$N_G(H)$的一个正规子群。证明如下：

任取$z\in Z_G(H)$，$g\in N_G(H)$。对H中任一个元素h，都有

$$(g^{-1}zg)^{-1}h(g^{-1}zg)=g^{-1}z^{-1}ghg^{-1}zg$$
$$=g^{-1}z^{-1}(ghg^{-1})zg.$$

因为$g\in N_G(H)$，所以$ghg^{-1}\in H$。因此z与ghg^{-1}可交换。于是

$$(g^{-1}zg)^{-1}h(g^{-1}zg)=g^{-1}(ghg^{-1})g=h.$$

由$Z_G(H)$的定义，知$g^{-1}zg\in Z_G(H)$。因此$Z_G(H)\trianglelefteq N_G(H)$。

判别条件五　G的子群H是正规子群的一个充分必要条件是：如果h在H中，那么H一定包含h在G中的一切共轭元素。即：H由一些共轭元素类组成。

证明　设$H\trianglelefteq G$。任取$h\in H,x\in G$，则由$x^{-1}Hx=H$可得$x^{-1}hx\in H$。因此H包含h的一切共轭元素。这就证明了条件的必要性。

如果对任一个$h\in H$，H都包含h在G中的一切共轭元素，那么对任一$x\in G$，都有$x^{-1}hx\in H$，于是$x^{-1}Hx\leqslant H$。另一方面，对于x^{-1}来说，有$(x^{-1})^{-1}Hx^{-1}\leqslant H$，即$xHx^{-1}\leqslant H$。由此得$H\leqslant x^{-1}Hx$。因此必须有$x^{-1}Hx=H$。所以$H\trianglelefteq G$。条件的充分性得证。▌

例7　由$(1,2,3,4,5)$生成的5阶循环群H是S_5的一个循环子群，但不是S_5的正规子群。因为$(1,2,3,4,5)$在S_5中一共有24个共轭元素，不能都在H中。所以H在S_5中不是正规的。

例8　四元数群G的阶等于8，所以它的非平凡子群的阶只可能等于2或4。前面已经看到G只有一个2阶子群，所以这个子群是G的正规子群。而G的4阶子群在G中的指数等于2，所以这一类子群也都是正规的。

四元数群给出了一个非交换群，它的子群都是正规子群

的例子。这样的群通常称为**哈密尔顿群**。四元数群是哈密尔顿群的一个特例。

最后我们举例说明一点需要注意的地方。正规子群没有传递性，即可能有下述情况：

$$G > G_1 > G_2,$$

其中

$$G \rhd G_1, \quad G \rhd G_2,$$

但是G_2不是G_1的正规子群。

例9 令

$G = A_4$,

$G_1 = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$,

$G_2 = \{e, (1,2)(3,4)\}$。

则

$$G \rhd G_1, \quad G_1 \rhd G_2.$$

但是，由于

$$(1,2,3)^{-1}G_2(1,2,3) = \{e, (1,4)(2,3)\} \neq G_2,$$

所以G_2不是G的正规子群。

我们以正规子群的一个重要性质来结束这一节。

如果A是G的一个子群，H是G的一个正规子群，那么

1) $A \cap H$是A的正规子群。

2) $AH = \{ah \mid a \in A, h \in H\}$是$G$的一个子群，而且$AH = HA$。

我们把证明留给读者作为练习。

§4 商群 同态定理

上一节我们证明了同态映射的核一定是正规子群，我们把所得的结果写成一个定理。

定理5（第一同态定理） 群G到G_1的同态映射φ的核K是G的一个正规子群。G中两个元素在φ下的象相同的充分必要条件是它们属于G的同一个陪集。

现在进一步来证明每个正规子群都可以作为某个同态映射的核。

设H是G的一个正规子群。G对H的陪集分解为

$$G = Hx_1 \cup Hx_2 \cup \cdots \cup Hx_r,$$

其中$Hx_1 = H$。

根据定理5，如果H是G到某个群G_1上的同态映射φ的核，那么G_1的阶等于r，而且G_1的r个元素就是

$$x_1^\varphi, x_2^\varphi, \cdots, x_r^\varphi.$$

其中$x_1^\varphi = e_1$是G_1的单位元素。又因为φ是保持运算的。所以G_1中的运算应该是

$$x_i^\varphi x_j^\varphi = (x_i x_j)^\varphi.$$

为了证明H是某个同态映射的核，我们需要证明满足上述条件的群是存在的。下面我们就来构作一个这样的群。

取正规子群H的r个陪集为元素，作一个集合F：

$$F = \{Hx_1, Hx_2, \cdots, Hx_r\}.$$

在F中定义一个乘法如下：

$$Hx_i Hx_j = Hx_i x_j.$$

因为H是正规子群，所以这个乘法事实上就是两个群子群的乘法，是与陪集代表的取法无关的。因此这样定义的运算是合理的。

下面来验证F对这样定义的乘法成一个群。

1) 结合律成立

$$(Hx_i Hx_j)Hx_k = (Hx_i x_j)Hx_k = H(x_i x_j)x_k$$

$$= Hx_i(x_jx_k) = Hx_iHx_jx_k$$
$$= Hx_i(Hx_jHx_k).$$

2) Hx_1就是F的单位元素。

3) 如果$x_i^{-1} \in Hx_l$，那么

$$Hx_iHx_l = Hx_iHx_i^{-1} = H = Hx_1.$$

故 $$(Hx_i)^{-1} = Hx_i^{-1}.$$

这说明F中元素都有逆元素。因此，F成为一个群，称为G对H的商群。

定义6 设H是G的一个子群。H在G中的全部陪集对群子集的乘法成一个群，称为G关于H的**商群**，记作G/N。

定理 6（第二同态定理） 设H是G的一个正规子群，G/H是G关于H的商群。那么G到G/H上的映射φ：

$$g \mapsto Hg$$

是一个满同态映射，其核为H。

证明 显然φ是映上的。为了证明φ是一个同态映射，只要证明φ保持运算就可以了。

对于G中任意两个元素g_1, g_2，我们有

$$(g_1g_2)^\varphi = Hg_1g_2 = Hg_1Hg_2 = g_1^\varphi g_2^\varphi.$$

因此φ保持运算，是一个同态映射。

最后来计算φ的核。核是G/H的单位元素的原象。因为G/H的单位元素是$Hx_1 = H$，又因

$$g^\varphi = H \rightleftharpoons Hg = H \rightleftharpoons g \in H,$$

所以φ的核就是H。 ▎

定理 6 中规定的同态映射φ称为G到商群G/N的**自然同态**。

以上我们证明了G的每个正规子群都可作为某个同态映射的核，而且每个商群都是G的同态象。下面来证明G的每个同态象都可这样得到，即：G的每个同态象都与G的某一个商群同构。这样，G的全部同态象就都可以由G的商群给出。

定理7（第三同态定理） 如果

$$\varphi: G \mapsto G_1$$

是一个满同态映射，φ的核是K。那么$G_1 \cong G/K$。

证明 设 $G = Kx_1 \cup Kx_2 \cup \cdots \cup Kx_r$.

则 $$G/K = \{Kx_1, Kx_2, \cdots, Kx_r\}.$$

根据第一同态定理，Kx_i中的元素在φ下的象都等于x_i^φ，因此可以定义商群G/N到G_1上的映射ρ：

$$Kx_i \mapsto x_i^\varphi.$$

很容易看出这个映射是一个一一对应，而且是保持运算的：

$$(Kx_iKx_j)^\rho = (Kx_ix_j)^\rho = (x_ix_j)^\varphi = x_i^\varphi x_j^\varphi$$
$$= (Kx_i)^\rho(Kx_j)^\rho.$$

因此ρ是一个同构映射。这就证明了

$$G_1 \cong G/K. \quad ▎$$

这样，我们就完全解决了群G的同态象的问题。我们把所得到的结论综述如下：

群G的任一同态映射的核都是G的正规子群；群G的任一个正规子群都是G的同态映射的核，而且以G的同一个正规子群为核的同态象都与G关于这个正规子群的商群同构，因此在同构的意义下是唯一的。

我们给出关于正规子群的一个重要定理。

定理 8（同构定理） 设A是G的一个子群，H是G的一个正规子群。那么有

$$AH/H \cong A/A \cap H.$$

证明 AH/H中的元素都可表成aH $(a \in A)$。如果

$aH=a'H(a,a'\in A)$，那么$a^{-1}a'\in A\cap H$。所以AH/H中每个元素都唯一决定$A/A\cap H$中一个元素。我们可以定义AH/H到$A/A\cap H$上的一个映射φ:

$$aH\mapsto a(A\cap H).$$

很明显，映射φ是一个同态映射。下面来求φ的核。

如果aH属于φ的核，那么它在φ下的象$a(A\cap H)$就是$A/A\cap H$的单位元素$A\cap H$。因此$a\in A\cap H$，从而$aH=H$。即φ的核只包含一个单位元素H。因此φ是一个同构映射。这就证明了

$$AH/H\cong A/A\cap H. \quad \blacksquare$$

最后，我们来举几个例子。

例10 设G是四元数群，$H=\{e,a^2\}$。已知H是G的正规子群，现在来求G关于H的商群。因为

$$G=H\cup Ha\cup Hb\cup Hab.$$

所以
$$G/H=\{H,Ha,Hb,Hab\}.$$

G/H中的运算如下表：

	H	Ha	Hb	Hab
H	H	Ha	Hb	Hab
Ha	Ha	H	Hab	Hb
Hb	Hb	Hab	H	Ha
Hab	Hab	Hb	Ha	H

所以G/H是4阶交换群，其中非单位元素都是2阶元素。

例11 $G=S_4$，

$$H=\{e,(1,2)(2,4),(1,3)(2,4),(1,4)(2,3)\}.$$

已知$H\lhd G$，来计算G/H。由G对H的陪集分解，知

$$G/H=\{H,H(1,2),H(1,3),H(2,3),H(1,2,3),H(1,3,2)\}.$$

因为当H是正规子群时，有$Ha\cdot Hb=Hab$。因此知

$$G/H\cong S_3.$$

还可看出，如果S_3表示$\{1,2,3\}$上的对称群，那么

$$G=HS_3=S_3H.$$

例12 G及H同例11。再令

$$A=\{e,(1,2,3,4),(1,3)(2,4),(1,4,3,2)\}.$$

则
$$AH=\{e,(1,3),(2,4),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3),(1,2,3,4),(1,4,3,2)\}<G.$$

$$A\cap H=\{e,(1,3)(2,4)\}<G.$$

$$AH/H=\{H,H(1,3)\}<G/H.$$

$$A/A\cap H=\{A\cap H,(A\cap H)(1,2,3,4)\}.$$

AH/H与$A/A\cap H$都是2阶循环群，所以

$$AH/H\cong A/A\cap H.$$

下列映射是AH/H到$A/A\cap H$上的一个同构映射：

$$H\mapsto A\cap H,\quad H(1,3)\mapsto(A\cap H)(1,2,3,4).$$

§5 A_n $(n\neq 4)$的单性

对于任意一个群G，它的平凡子群$\{e\}$及G都是正规子群。除了这两个平凡子群之外，如果G不再包含其它正规子群，G就称为一个**单群**。

当G是交换群的时候，任一个子群都是正规子群，所以G是否是单群就根据G是不是有非平凡子群而决定。因此可以用G的阶来判断。

定理9 有限交换群G是单群的充分必要条件是G的阶是一个素数。

证明 条件的充分性是明显的，因为根据拉格朗日定理，G的子群的阶必须是$|G|$的因数。现在来证条件的必要性。设G的阶不是一个素数，在G中取定一非单位元素a。如果a的阶小于G的阶，那么a生成的循环群就是G的一个非平凡子群。如果a的阶等于G的阶，取$|G|$的一个眞因数k：

$$1<k<|G|.$$

令

$$b=a^k.$$

那么b是G中一个阶小于$|G|$的非单位元素，$\langle b\rangle$就是G的一个非平凡子群。 ▌

非交换的单群也是存在的。这一节的主要內容就是证明交错群$A_n(n\neq 4)$都是单群。

为此，我们首先需要讨论A_n的构造。

引理 A_n $(n\geqslant 3)$由一切长度为3的轮换生成。

证明 A_n中每个元素都是偶置换，因此都可以表成偶数个对换的乘积。两个不相同的对换如果有一个公共文字，那么它们的乘积就等于一个3-轮换：

$$(\alpha,\beta)(\alpha,\gamma)=(\alpha,\beta,\gamma).$$

如果它们沒有公共文字，那么它们的乘积可以表成两个3-轮换的乘积：

$$(\alpha,\beta)(\gamma,\delta)=(\alpha,\beta,\gamma)(\alpha,\delta,\gamma).$$

所以A_n中每个元素都可表成3-轮换的乘积。

另一方面，长度为3的轮换都是偶置换，故都在A_n中。

总结这两方面，就得到所要证明的结论。 ▌

定理10 A_n $(n\neq 4)$是单群。

证明 当$n=2$时，$A_2=\{e\}$。当$n=3$时，A_3是3阶循环群，因此都是单群。下面对$n\geqslant 5$的情形来证明。

设H是A_n $(n\geqslant 5)$的一个正规子群，并设$H\neq\{e\}$。来证明$H=A_n$。

如果H包含一个3-轮换(α,β,γ)，我们来证明H一定包含任一个3-轮换$(\bar\alpha,\bar\beta,\bar\gamma)$。作$n$元置换

$$\tau=\begin{pmatrix}\alpha & \beta & \gamma & \delta & \varepsilon & \cdots\\ \bar\alpha & \bar\beta & \bar\gamma & \bar\delta & \bar\varepsilon & \cdots\end{pmatrix}.$$

可以适当地调动$\bar\delta,\bar\varepsilon$的次序使$\tau$是一个偶置换。因此$\tau\in A_n$。$\tau$具有下述性质：

$$\tau^{-1}(\alpha,\beta,\gamma)\tau=(\bar\alpha,\bar\beta,\bar\gamma).$$

因为H是A_n的正规子群，所以$(\bar\alpha,\bar\beta,\bar\gamma)\in H$。由引理即得

$$H=A_n.$$

现在来证明H中一定有3-轮换。

我们称一个置换所实际变动的文字个数为这个置换的次数。在H中取定一个次数最小的非单位元素，设为σ。因为σ是偶置换，所以σ的次数至少是3。我们来证σ的次数恰等于3，因此是一个长度为3的轮换。

我们用反证法来证明这个结论。如果σ的次数大于3，那么在它的轮换表法的省略形式中至少出现4个文字。因此σ或者是一些不相交的对换的乘积：

$$\sigma=(\alpha,\beta)(\gamma,\delta)\cdots,$$

或者包含一个长度不小于3的轮换

$$\sigma=(\alpha,\beta,\gamma,\cdots).$$

这时σ至少变动5个文字，否则$\sigma=(\alpha,\beta,\gamma,\delta)$将是一个奇置换，不可能在$A_n$中。

在第一种情形，令$\tau=(\gamma,\delta,\varepsilon)$。再令

$$\sigma_1=\tau^{-1}\sigma\tau=(\alpha,\beta)(\delta,\varepsilon)\cdots.$$

在第二种情形，设 δ,ε 是 σ 变动的另两个文字。令 $\tau=(\gamma,\delta,\varepsilon)$，则得

$$\sigma_1=\tau^{-1}\sigma\tau=(\alpha,\beta,\delta,\cdots)\cdots.$$

在这两种情形，都有 $\sigma_1\neq\sigma$。因此 $\sigma_1\sigma^{-1}\neq e$。而因$H$是正规子群，故有$\sigma_1\sigma^{-1}\in H$。但是$\sigma_1\sigma^{-1}$的次数比$\sigma$的次数少，这与$\sigma$的取法相矛盾。所以 σ 一定是一个 3-轮换。从而

$$H=A_n. \quad \blacksquare$$

当$n=4$时，我们已知 A_4有一个 4 阶正规子群，所以 A_4 不是单群。

定理11 A_n $(n\neq4)$是S_n的唯一的非平凡正规子群。

证明 设H是S_n的一个非平凡正规子群。H中全部偶置换组成H的一个指数为 2 的正规子群H^+。$H^+=H\cap A_n$是A_n的一个正规子群。由A_n的单性，知 $H^+=A_n$或$H^+=\{e\}$。如果H^+是单位子群，那么H是一个 2 阶子群，由恒等置换和一个奇置换组成，不可能是S_n的正规子群。所以 $H^+=A_n$，$H\geqslant A_n$。又因H是S_n的真子群，所以$H=A_n$。 $\blacksquare$

交错群是一类很重要的单群，其中A_5是阶数最小的非交换单群。Galois理论利用$A_n(n\geqslant5)$的单性成功地证明了五次和五次以上的一元代数方程不能用根式来求解。

§6 自同构群

6.1 自同构群

群G到它自身的同构映射称为G的**自同构**。自同构的一个最简单的例子就是恒等映射，称为**恒等自同构**。在恒等自同构下，群中每个元素都保持不变。下面再来举几个自同构的例子。

例1 用$\mathbf{Z}$表整数加法群，将整数 n 映到 $-n$ 的映射是 $\mathbf{Z}$ 的一个自同构。

例2 设G是一个交换群，将G的每个元素映到其逆元素的映射：

$$a\mapsto a^{-1},\quad a\in G$$

是G的一个自同构。

这个例子包含例 1 作为特例。如果G中包含阶不等于 1 或 2 的元素，那么这个自同构不是恒等自同构。

例3 设G是一个群，a 是G中一个取定的元素。定义映射φ_a:

$$x\mapsto x^{\varphi_a}=a^{-1}xa,\qquad x\in G.$$

这个映射是一个一一映射，而且是保持运算的：

$$(xy)^{\varphi_a}=a^{-1}(xy)a=(a^{-1}xa)(a^{-1}ya)$$
$$=x^{\varphi_a}y^{\varphi_a}.$$

所以φ_a是G的一个自同构。这样的自同构称为**内自同构**。一个自同构如果不是内自同构，就称为**外自同构**。

自同构是群到自身的同构映射，因此与同构映射一样，有下述一些性质。

1）自同构将单位元素映到单位元素。

2）自同构将一个元素的逆元素映到这个元素的象的逆元素。

3）自同构将中心元素映到中心元素。

因此，如果用Z表群G的中心，那么对G的任一自同构φ，都有

$$Z^{\varphi}=Z.$$

4）如果H是G的一个子群，φ是 G的一个自同构，那

么H的象集合

$$H^{\varphi}=\{h^{\varphi}\mid h\in H\}$$

也是G的一个子群。当然H与H^{φ}是同构的。

5）如果$H\trianglelefteq G$，那么$H^{\varphi}\trianglelefteq G$。

证明 任取$g\in G,h\in H^{\varphi}$。设g_1是g的原象，h_1是h的原象，即$g_1^{\varphi}=g$，$h_1^{\varphi}=h$。那么

$$g^{-1}hg=(g_1^{\varphi})^{-1}h_1^{\varphi}g_1^{\varphi}=(g_1^{-1})^{\varphi}h_1^{\varphi}g_1^{\varphi}$$
$$=(g_1^{-1}h_1g_1)^{\varphi}.$$

因此$h_1\in H$而$H\trianglelefteq G$，所以$g_1^{-1}h_1g_1\in H$，因此$g^{-1}hg\in H^{\varphi}$，H^{φ}是G的一个正规子群。∎

如果φ_1,φ_2是G的两个自同构，那么它们的乘积$\varphi_1\varphi_2$也是G的自同构。又G的自同构的逆映射也是G的自同构。用$A(G)$表示G的全部自同构组成的集合，则$A(G)$对映射的乘法构成一个群，称为G的**自同构群**。恒等自同构是$A(G)$的单位元素。

例4 设$G=\{e,a\}$是一个2阶循环群，那么G只有一个自同构，即恒等自同构。所以$A(G)$是由一个单位元素组成的群。2阶群是唯一的除恒等自同构外不再有其他自同构的群。

例5 $G=\{e,a,b,c\}$是4阶非循环交换群。G中运算为

$$a^2=b^2=c^2=e,\qquad ab=ba=c,$$
$$ac=ca=b,\qquad bc=cb=a.$$

我们来计算它的自同构群。

如果φ是G的一个自同构，那么φ必须把e映到e，而把a,b,c分别映到a,b,c中的某一个，而且各不相等。因此，φ的作用有下述六种可能：

$$\varphi_1:\ e,a,b,c\mapsto e,a,b,c;$$
$$\varphi_2:\ e,a,b,c\mapsto e,a,c,b;$$
$$\varphi_3:\ e,a,b,c\mapsto e,b,a,c;$$
$$\varphi_4:\ e,a,b,c\mapsto e,b,c,a;$$
$$\varphi_5:\ e,a,b,c\mapsto e,c,a,b;$$
$$\varphi_6:\ e,a,b,c\mapsto e,c,b,a.$$

很容易验证这六个映射都是G的自同构。所以G的自同构群一共包含6个元素：

$$A(G)=\{\varphi_1,\varphi_2,\varphi_3,\varphi_4,\varphi_5,\varphi_6\},$$

其中φ_1是恒等自同构。

从φ_i（$i=1,2,\cdots,6$）的作用还可看出：$A(G)\cong S_3$。

例6 试证：S_3共有6个自同构，都是内自同构，而且S_3的自同构群与S_3同构。

证明 如果φ是S_3的一个自同构，那么φ将S_3中的2阶元素映到2阶元素。因此，φ将$(1,2),(1,3),(2,3)$这3个元素作置换。因为这3个元素生成S_3，所以S_3的自同构被它在这3个2阶元素上的作用唯一确定。这说明S_3最多有6个自同构。考虑S_3的内自同构。如果S_3中两个元素σ,τ所对应的内自同构相同：$\varphi_\sigma=\varphi_\tau$，则对$S_3$中任一个元素$x$，都有

$$\sigma^{-1}x\sigma=\tau^{-1}x\tau.$$

于是
$$x(\sigma\tau^{-1})=(\sigma\tau^{-1})x.$$

$\sigma\tau^{-1}$是S_3的中心元素。但是S_3是无中心群，所以$\sigma\tau^{-1}=e$，即$\sigma=\tau$。这样，S_3恰有6个内自同构。因而S_3的6个自同构都是内自同构，其自同构群为

$$A(S_3)=\{\varphi_e,\varphi_{(1,2)},\varphi_{(1,3)},\varphi_{(2,3)},\varphi_{(1,2,3)},$$
$$\varphi_{(1,3,2)}\}.$$

容易证明，S_3到$A(S_3)$上的映射

$$x\mapsto\varphi_x$$

是一个同构映射。因此$S_3 \cong A(S_3)$。

如果群G是无中心群，并且G的自同构都是内自同构，就称G是一个**完全群**。例6说明S_3是一个完全群。事实上，只要$n \geqslant 3$且$n \neq 6$，S_n都是完全群。这一结论我们在这里不予证明。

要找出一个已知群的自同构群一般是很困难的。在大多数情形下，群本身的性质不能转移到它的自同构上去。例如，例5说明一个交换群的自同构群可以是非交换的。例5和例6说明不同构的群可能有同构的自同构群。

可以断定，一个有限群的自同构群一定也是一个有限群。因为群G的自同构将G的元素作置换，所以G的自同构群可以看成作用于G上的置换群，而且因为每个自同构都把单位元素保持不变，因此，如果G的阶为n，那么$A(G)$可以看成是S_{n-1}的一个子群。例5给出一个例子说明存在n阶群G使$A(G)$等于S_{n-1}。

6.2 内自同构群

群G的两个内自同构的乘积还是一个内自同构：

$$\varphi_a \varphi_b = \varphi_{ab},$$

而且内自同构的逆映射也是内自同构：

$$(\varphi_a)^{-1} = \varphi_{a^{-1}},$$

所以G的内自同构全体组成G的自同构群$A(G)$的一个子群，记作$I(G)$，称为G的**内自同构群**。

内自同构群有下述一些性质。

1) G到内自同构群$I(G)$上的映射

$$a \mapsto \varphi_a, \quad a \in G$$

是一个同态映射，其核为G的中心$Z(G)$，所以

$$I(G) \cong G/Z(G).$$

2) 设a,b是G的两个元素，那么

$$\varphi_a = \varphi_b \Leftrightarrow Z(G)a = Z(G)b.$$

3) $I(G)$是$A(G)$的一个正规子群。

证明 设σ是G的一个自同构，φ_a是G的一个内自同构。则对G中任一元素x，x在$\sigma^{-1}\varphi_a\sigma$下的象为

$$x^{\sigma^{-1}\varphi_a\sigma} = (x^{\sigma^{-1}})^{\varphi_a\sigma} = (a^{-1}x^{\sigma^{-1}}a)^{\sigma}$$

$$= (a^{\sigma})^{-1}xa^{\sigma} = x^{\varphi_{a^{\sigma}}}.$$

所以$\sigma^{-1}\varphi_a\sigma = \varphi_{a^\sigma}$也是一个内自同构。因此$I(G)$是$A(G)$的正规子群。▎

群G的自同构群关于内自同构群的商群$A(G)/I(G)$称为G的**外自同构群**。

6.3 特征子群

我们知道，如果H是G的一个子群，φ是G的一个自同构，那么H^{φ}也是G的一个子群。当然，一般地H^{φ}不一定与H相同。

定义 7 如果G的子群H在群的任一个自同构下的象都等于H，H就称为G的一个**特征子群**。

因为特征子群在内自同构下的象也等于自己，所以特征子群一定是正规子群。正规子群是在内自同构下保持不变的子群，所以正规子群也称**不变子群**。但是正规子群不一定是特征子群。这一点可以从下例看到。

例 7 我们已知四元数群G的子群都是正规子群。因为群的自同构保持元素的阶不变，而G中只有一个2阶元素a^2，所以子群$\{e,a^2\}$是G的一个特征子群。但是子群

$$\langle b\rangle=\{e,b,a^2,a^2b\}$$

就不是特征子群。因为$\langle b\rangle$在下述自同构下的象不等于$\langle b\rangle$。

令φ为G到自身的映射：

$$e\mapsto e,\quad a\mapsto a,\quad a^2\mapsto a^2,\quad a^3\mapsto a^3,$$

$$b\mapsto ab,\quad ab\mapsto a^2b,\quad a^2b\mapsto a^3b,\quad a^3b\mapsto b.$$

那么，φ是G的一个自同构(请读者自己验证)。而

$$\langle b\rangle^{\varphi}=\{e,ab,a^2,a^3b\}.$$

因为群的自同构把中心映到中心，所以群G的中心Z是G的特征子群。

我们在以前曾经举例说明过，正规子群这个性质不是可传的。而一个子群是特征子群这一性质却是可传的：如果G_1是G的特征子群，G_2是G_1的特征子群，那么G_2一定是G的特征子群。这是因为：G的任一个自同构φ把G_1映到它自身，因此可以看成是G_1的一个自同构。又由于G_2是G_1的特征子群，所以$G_2^{\varphi}=G_2$。

但是要注意：如果

$$G>G_1>G_2,$$

而且G_2是G的一个特征子群，这时G_2有可能不是G_1的特征子群。我们举例说明这一事实。

例 8 设G是由a,b,c三个元素生成的有限群，G中元素的运算满足

$$a^3=b^3=c^3=e,\quad ab=bac,$$

$$ac=ca,\quad bc=cb.$$

因此，G中元素可表成

$$a^kb^lc^m,\quad 0\leqslant k,l,m<3.$$

G是一个27阶非交换群。G的中心Z是由c生成的3阶子群。Z是G的一个特征子群。

用G_1表示G的由a,c生成的子群。G_1是一个9阶非循环交换群：

$$G>G_1>Z.$$

G_1中元素可表成

$$a^kc^l,\quad 0\leqslant k,l<3.$$

映射φ：

$$a^kc^l\mapsto a^lc^k$$

是G_1的一个自同构。因为

$$Z^{\varphi}=\langle a\rangle\neq Z,$$

所以Z不是G_1的特征子群。

6.4 换位子群

这一 我们介绍一类重要的特征子群。

定义 设G是一个群，a,b是G中两个元素，元素$a^{-1}b^{-1}ab$称为a,b的**换位元素**。由G的全部换位元素生成的子群称为G的**换位子群**，或称**导群**。

我们常用$[a,b]$表示a,b的换位元素，而用$[G,G]$或G'表示G的换位子群。

需要注意的是，G的导群G'是由G中换位元素生成的子群。一般来说，G的全体换位元素不一定组成一个子群。因此，G'中的元素是一些换位元素的乘积，但不一定都是换位元素。

因为对于G的任一自同构φ，都有

$$[a,b]^{\varphi}=(a^{-1}b^{-1}ab)^{\varphi}=(a^{\varphi})^{-1}(b^{\varphi})^{-1}a^{\varphi}b^{\varphi}$$
$$=[a^{\varphi},b^{\varphi}].$$

所以G'是G的一个特征子群。

容易看出，G中两个元素a,b可交换的充分必要条件是

它们的换位元素$[a,b]=e$。当G是交换群的时候，$G'=\{e\}$。这也是G为交换群的一个充分条件。我们有下述更为一般的结果。

定理11 1) G关于换位子群G'的商群G/G'是交换的。

2) 如果H是G的一个正规子群，那么当且仅当$H\geqslant G'$时，商群G/H是交换的。

证明 1) 对于G中任意两个元素a,b，来证$G'a$与$G'b$可交换。因为它们的换位元素是

$$
\begin{aligned}
&(G'a)^{-1}(G'b)^{-1}(Ga)(Gb)\\
&=G'a^{-1}\cdot G'b^{-1}\cdot G'a\cdot G'b\\
&=G'a^{-1}b^{-1}ab=G'.
\end{aligned}
$$

所以$G'aG'b=G'b\cdot G'a$。即G/G'是交换的。

2) G/H是交换群的涵意是对G中任意两个元素a,b，都有

$$(Ha)(Hb)=(Hb)(Ha).$$

这个条件等价于

$$(Ha)^{-1}(Hb)^{-1}(Ha)(Hb)=H.$$

即
$$Ha^{-1}b^{-1}ab=H.$$

亦即
$$a^{-1}b^{-1}ab=[a,b]\in H.$$

因此当且仅当$H\geqslant G'$时，G/H是交换的。 ▎

例 8 交错群A_4的不同的换位元素共有4个：

$$e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3).$$

这4个元素组成一个子群，即A_4'。

例 9 在对称群S_4中，任一偶置换都是换位元素。另一方面，凡是换位元素一定是偶置换。所以S_4的换位子群就是A_4。

这个结论对一切n都成立。S_n的换位子群是A_n，而且A_n中的元素都是换位元素。

因为G的换位子群G'是G的正规子群，因此当G是非交换单群时，$G'=G$。由此可知，A_n的换位子群就等于A_n。

习 题

1. 求四元数群的全部互不同构的同态象。

2. 设φ是群G到群H上的一个满同态映射，A是G的一个子群。试证：如果A的阶与H的阶互素，那么A包含在φ的核中。

3. 试证：共轭元素的中心化子是共轭的。

4. 试证：共轭元素的正规化子是共轭的。

5. 证明：如果有限群G只有两个共轭元素类，那么G的阶等于2。

6. 如果H是有限群G的一个真子群，那么G中必有元素不属于H的任一个共轭子群。

7. 设σ，τ是对称群S_n中两个元素，证明：σ，τ在S_n中共轭的充分必要条件是它们的轮换表法中轮换的个数相同，而且可以排列轮换的次序，使得对应的轮换长度相同(这样的置换称作是同型的)。

8. 证明：如果n元置换σ的轮换表法中有m_1个1-轮换，m_2个2-轮换，…，m_n个n-轮换，则σ在S_n内的中心化子的阶等于

$$\prod_k k^{m_k}\cdot m_k!\quad(\text{规定}0!=1).$$

9. 设$G=\{e,(a_1,a_2,a_3),(a_1,a_3,a_2),(a_4,a_6)(a_5,a_7),$
$(a_1,a_2,a_3)(a_4,a_6)(a_5,a_7),$

$(a_1, a_3, a_2)(a_4, a_6)(a_5, a_7)$,

$(a_1, a_2)(a_4, a_5, a_6, a_7)$,

$(a_1, a_2)(a_4, a_7, a_6, a_5)$,

$(a_1, a_3)(a_4, a_7, a_6, a_5)$,

$(a_2, a_3)(a_4, a_7, a_6, a_5)\}$

是S_7的一个子群。

(1) 求G在S_7内的中心化子Z及正规化子N。

(2) 验证$Z \lhd N$。

10．证明：正规子群的交是正规子群。

11．证明：如果A, B都是G的正规子群，那么AB也是G的正规子群。

12．设A, B都是群G的正规子群，并设它们的阶互素。试证：A中任一元素与B中任一元素都可交换。

13．设H是群G的一个正规子群，a是G中一个元素。试证：如果a的阶与H在G中的指数互素，则$a \in H$。

14．设H是G的一个正规子群，A是G的一个子群。试证：

(1) 如果A的阶与H在G中的指数互素，则$HA = H$。

(2) 如果A在G中的指数与H的阶互素，则$HA = A$。

15．如果群G有一个交换的正规子群H包含于G的中心，并且G/H是循环群，那么G是交换群。

16．试证：群G的循环正规子群的子群仍是G的正规子群。

17．如果H是G的正规子群，则$G/H \cong S_{G/H}$。

18．设φ是G到G_1的一个满同态，H是G的一个正规子群。求证：

(1) H^φ是G_1的正规子群。

(2) $G/H \cong G_1/H^\varphi$。

19．如果H和K都是群G的正规子群，并且$K \leqslant H$，则

$$G/H \cong G/K \Big/ G/H.$$

因此还有

$$G/K \sim G/H.$$

20．G是一个群。证明：G是交换群的充分必要条件是G到自身的映射

$$a \mapsto a^{-1}, \quad a \in G$$

是G的一个自同构。

21．设G是一个n阶循环群。

(1) 求G的自同构群$A(G)$。

(2) 证明：如果n是一个素数，则$A(G)$是一个循环群。

22．设a, b是群G的两个元素。试证：

(1) 如果a与$[a, b]$可交换，则对任意正整数n，都有

$$[a^n, b] = [a, b]^n.$$

(2) 如果a, b都与$[a, b]$可交换，则对任意正整数n，都有

$$[a, b]^n = a^n b^n [b, a]^{\binom{n}{2}}.$$

23．已知$H = \langle a \rangle$是四元数群G的一个正规子群，证明H不是G的特征子群。

24．证明循环群的子群都是特征子群。

25．如果H是G的正规子群，A是H的特征子群，试证：A是G的正规子群。

第三章 置 换 群

因为每个抽象群都与一个置换群同构，所以从代数结构来看，这两类群是沒有什么差别的。然而，有些关于置换群的概念，例如不动点和传递性等概念以及由此而得出的置换群的一些特殊子群等，是置换群所独有的。而且我们还可以很方便地利用置换群来构造一般群。此外，置换群在其它学科中也有很好的应用。因此我们有必要对置换群进行独立的研究。

这一章对置换群作初步的讨论。

§1 置换群的一些子群

在这一章中，我们用G表示n元集合$\Omega=\{a_1,a_2,\cdots,a_n\}$上的一个置换群。$\Omega$中的文字称为点。如果$g$是$G$中的一个元素，用$a^g$表示$a$在$g$下的象。即

$$g=\begin{pmatrix}a_1 & a_2 & \cdots & a_n\\ a_1^g & a_2^g & \cdots & a_n^g\end{pmatrix}=\begin{pmatrix}a\\ a^g\end{pmatrix}.$$

这一节介绍置换群的一些子群。

1.1 稳定子群G_a

取定Ω中一个点a，用G_a表示G中保持a不变的全部置换所成的集合，用a^G表示a在G中置换作用下的象集合：

$$G_a=\{g\in G\,|\,a^g=a\};$$

$$a^G=\{a^g\,|\,g\in G\}.$$

定理 1 G_a是G的一个子群，G_a的阶满足等式

$$|G|=|G_a|\,|a^G|.$$

证明 首先来证G_a是一个子群。G_a当然不是一个空集，因为恒等置换一定属于G_a。如果g_1与g_2都在G_a中，

那么 $$a^{g_1}=a^{g_2}=a.$$

因此 $$a^{g_1g_2}=a.$$

所以$g_1g_2\in G_a$。G_a是G的一个子群。

为了计算G_a的阶，我们讨论G对G_a的陪集分解。

设 $$a^G=\{a=a_1,a_2,\cdots,a_r\},$$

幷设 $$a_i=a^{g_i},g_i\in G,\ i=1,2,\cdots,r.$$

则有 $$G=G_ag_1\cup G_ag_2\cup\cdots\cup G_ag_r.$$

这一点可如下证明。

陪集$G_ag_i(i=1,2,\cdots,r)$中每个置换都把a映到a_i，所以陪集$G_ag_1,G_ag_2,\cdots,G_ag_r$各不相同。下面证明$G$中每个元素都必属于这些陪集中的一个。任取$g\in G$，那么$a^g\in a^G$。设$a^g=a_k,1\leqslant k\leqslant r$。则

$$a^g=a^{g_k},\quad gg_k^{-1}\in G_a,\quad g\in G_ag_k.$$

这就证明了上述陪集分解式。从这个陪集分解式就可得出等式

$$|G|=|G_a|\,|a^G|.$$

定理证毕。▎

G_a称为G对a的**稳定子群**。

如果$a^g=a$，则称a是g的一个**不动点**。关于不动点和稳定子群，有下述一些简单性质。

引理 1 设h及g都是Ω上的置换，$a\in\Omega$。如果a是h的不动点，那么a^g是$g^{-1}hg$的不动点。

证明 根据假设，有

$$(a^g)^{g^{-1}hg}=a^{hg}=a^g.$$

所以a^g是$g^{-1}hg$的不动点。 ▎

引理 2 设G是Ω上一个置换群，$g\in G,a\in\Omega$。则

$$g^{-1}G_a g=G_{a^g}.$$

证明 由引理 1，知$g^{-1}G_a g\leqslant G_{a^g}$。另一方面，由引理 1 可得到

$$(g^{-1})^{-1}G_{a^g}g^{-1}\leqslant G_a.$$

因而$G_{a^g}\leqslant g^{-1}G_a g$。所以$g^{-1}G_a g=G_{a^g}$。 ▎

定理 2 1）如果$a^G=\{a=a_1,a_2,\cdots,a_r\}$，则与$G_a$共轭的子群一定是下述子群之一：

$$G_{a_1},G_{a_2},\cdots,G_{a_r}\text{（其中可能有相同的）。}$$

2）如果G_a在$a_1,a_2,\cdots,a_r$中共有t个不动点，那么G_a一共有r/t个不同的共轭子群。

证明 根据G对G_a的陪集分解

$$G=G_ag_1\cup G_ag_2\cup\cdots\cup G_ag_r$$

$$(a^{g_i}=a_i,\ i=1,2,\cdots,r)$$

以及$G_a\leqslant N_G(G_a)$，可知G_a的共轭子群一定是

$$g_i^{-1}G_ag_i=G_{a^{g_i}}=G_{a_i}\quad(i=1,2,\cdots,r)$$

中的一个。

如果G_a还保持a_i（$a_i\in a^G$）不变，那么

$$G_a\leqslant G_{a_i}.$$

但是上面已经证明了G_a与G_{a_i}是共轭的，所以$G_a=G_{a_i}$。如果G_a在a^G中一共有t个不动点，不妨设为$a_1,a_2,\cdots,a_t$。那么就有

$$G_a=G_{a_2}=\cdots=G_{a_t}.$$

对于G_ag_i（$i=1,2,\cdots,r$）中任一元素h_i，都有

$$h_i^{-1}G_ah_i=G_ah_i=G_{a_i}.$$

所以 $\quad G_ag_i\leqslant N_G(G_a),\quad i=1,2,\cdots,t.$

而当$i=t+1,\cdots,r$时，G_ag_i中任一元素都不属于$N_G(G_a)$。因此

$$N_G(G_a)=G_a\cup G_ag_2\cup\cdots\cup G_ag_t.$$

于是 $\quad |N_G(G_a):G_a|=t,\quad |G:N_G(G_a)|=r/t.$

所以G_a共有r/t个共轭子群。 ▎

例 1 $G=\{e,(a_1,a_2),(a_1,a_3),(a_2,a_3),$
$(a_1,a_2,a_3),(a_1,a_3,a_2),(a_4,a_5),$
$(a_1,a_2)(a_4,a_5),(a_1,a_3)(a_4,a_5),$
$(a_2,a_3)(a_4,a_5),(a_1,a_2,a_3)(a_4,a_5),$
$(a_1,a_3,a_2)(a_4,a_5)\}.$

G是S_5的一个12阶子群。下面列出G_{a_i}（$i=1,2,\cdots,5$）及其共轭子群。

$$G_{a_1}=\{e,(a_2,a_3),(a_4,a_5),(a_2,a_3)(a_4,a_5)\};$$
$$G_{a_2}=\{e,(a_1,a_3),(a_4,a_5),(a_1,a_3)(a_4,a_5)\};$$
$$G_{a_3}=\{e,(a_1,a_2),(a_4,a_5),(a_1,a_2)(a_4,a_5)\};$$
$$G_{a_4}=G_{a_5}=\{e,(a_1,a_2),(a_1,a_3),(a_2,a_3),(a_1,a_2,a_3),(a_1,a_3,a_2)\}.$$

因为 $\quad a_1^G=a_2^G=a_3^G=\{a_1,a_2,a_3\},$

所以G_{a_1}，G_{a_2}，G_{a_3}组成一个共轭子群类。

又因 $\quad a_4^G=a_5^G=\{a_4,a_5\},$

而且 $\quad G_{a_4}=G_{a_5},$

因而G_{a_4}的共轭子群只有它自己。所以

$$G_{a_4}\lhd G.$$

1.2 G_Δ 和 $G_{(\Delta)}$

可以将稳定子群的概念加以推广。设 Δ 是 Ω 的一个非空子集，用 G_Δ 表示 G 中那些保持 Δ 中每个点都不变的置换所成的集合：

$$G_\Delta=\{g\in G\mid \alpha^g=\alpha,\quad \forall\alpha\in\Delta\}.$$

可以和前面一样证明 G_Δ 是 G 的一个子群。当 Δ 由一个点 α 组成时，G_Δ 就是 G_α。我们有

$$G_\Delta=\bigcap_{\alpha\in\Delta}G_\alpha\quad(\Delta\neq\varnothing),$$

$$G_{\Delta\cup\Gamma}=G_\Delta\cap G_\Gamma=(G_\Delta)_\Gamma.$$

由定理 1 可得下述有用公式：

$$|G:G_{\alpha\beta}|=|\alpha^G||\beta^{G_\alpha}|=|\beta^G||\alpha^{G_\beta}|.$$

用 Δ^g 表 Δ 在 g 下的象集。则 G_Δ 的共轭子群也有和 G_α 类似的性质：

$$g^{-1}G_\Delta g=G_{\Delta^g},$$

其中 g 是 G 中任意置换。特别地，如果对 G 中每个置换 g 都有 $\Delta^g=\Delta$，那么 $G_\Delta\trianglelefteq G$。

如果我们考虑 G 中那些保持集合 Δ 不变的置换，令

$$G_{(\Delta)}=\{g\in G\mid\Delta^g=\Delta\}.$$

那么 $G_{(\Delta)}$ 也是 G 的一个子群。由 G_Δ 及 $G_{(\Delta)}$ 的定义知

$$G_\Delta\leqslant G_{(\Delta)}.$$

不仅如此，我们还有下述结论。

定理3 G_Δ 是 $G_{(\Delta)}$ 的正规子群。

证明 任取 $g\in G_\Delta, h\in G_\Delta$，要证 $h^{-1}gh\in G_\Delta$。如果 α 是 Δ 中的一个点，那么因为 $h^{-1}\in G_{(\Delta)}$，故有

$$\alpha^{h^{-1}}\in\Delta.$$

因此 $$\alpha^{h^{-1}gh}=[(\alpha^{h^{-1}})^g]^h=(\alpha^{h^{-1}})^g=\alpha.$$

所以 $$h^{-1}gh\in G_\Delta,\quad G_\Delta\trianglelefteq G_{(\Delta)}.\ ▌$$

例2 对于例 1 中的 G，令 $\Delta=\{\alpha_1,\alpha_2\}$。则

$$G_\Delta=\{e,(\alpha_4,\alpha_5)\},$$

$$G_{(\Delta)}=\{e,(\alpha_1,\alpha_2),(\alpha_4,\alpha_5),(\alpha_1,\alpha_2)(\alpha_4,\alpha_5)\}.$$

很容易看出

$$G_\Delta\trianglelefteq G_{(\Delta)}.$$

§2 传 递 群

2.1 传 递 群

上一节我们讨论了 Ω 上置换群 G 的稳定子群，知道 G_α 的阶等于 $|G|/|\alpha^G|$，其中 $\alpha^G=\{\alpha^g\mid g\in G\}$。这一节进一步讨论 $\alpha^G=\Omega$ 的情形，这时，G 称为一个传递群。

定义1 G 是 $\Omega=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$ 上的一个置换群。如果对任一 $\alpha_i(i=1,2,\cdots,n)$ 都有 G 中一个元素 g_i 使 $\alpha_1^{g_i}=\alpha_i$，那么 G 就称为 **Ω 上的传递群**，简称**传递群**。如果 G 不是传递群，就称 G 为**非传递群**。

如果 $\alpha_1^{g_i}=\alpha_i$，$\alpha_1^{g_j}=\alpha_j$，那么置换 $g_i^{-1}g_j$ 将 α_i 映到 α_j：

$$\alpha_i^{g_i^{-1}g_j}=\alpha_1^{g_j}=\alpha_j.$$

因此，如果 G 在 Ω 上是传递的，那么对 Ω 中任意两个点 α_i，α_j 都可找到 G 中一个置换 g，使得

$$\alpha_i^g=\alpha_j.$$

例如，S_n 及 $A_n(n>2)$ 都是传递群；§1例1中的置换群不是传递群；任一群的正则表示以及群对子群的陪集置换表

示都是传递群。

对于传递群来说，任一 $a\in\Omega$ 都有

$$a^G=\Omega.$$

因此，我们可以将上一节中的结果用于传递群而得

定理4 设 G 是 $\Omega=\{a_1=a,a_2,\cdots,a_n\}$ 上的一个传递群，G_a 是 G 对 a 的稳定子群。则有

1) 任取 G 中将 a 映到 a_i 的一个置换 $g_i(i=1,2,\cdots,n)$，那么陪集 G_ag_i 由 G 中将 a 映到 a_i 的全体置换组成。而

$$G=G_a\cup G_ag_2\cup\cdots\cup G_ag_n.$$

2) $|G:G_a|=n$。

这说明 n 元传递群的阶一定是 n 的一个倍数。

定理5 G 是 n 元集合 Ω 上的传递置换群，$a\in\Omega$，如果 G_a 共有 t 个不动点，那么 G_a 共有 n/t 个共轭子群。

2.2 多重传递群

定义2 设 G 是 $\Omega=\{a_1,a_2,\cdots,a_n\}$ 上的一个置换群。如果对于 Ω 中任意 k 个点 $a_{i_1},a_{i_2},\cdots,a_{i_k}$，都有 G 中一个置换 g 使得

$$a_1^g=a_{i_1},a_2^g=a_{i_2},\cdots,a_k^g=a_{i_k},$$

那么就称 G 为 **k 重传递群**(或 **k-传递群**)。

和传递群一样，由 k 重传递群的定义可推出：对于 Ω 的任意两个 k 元子集 $a_{i_1},a_{i_2},\cdots,a_{i_k}$ 及 $a_{j_1},a_{j_2},\cdots,a_{j_k}$，都有 G 中一个置换 g 使得

$$a_{i_1}^g=a_{j_1},\quad a_{i_2}^g=a_{j_2},\quad\cdots,\quad a_{i_k}^g=a_{j_k}.$$

当然，传递群是 k 重传递群的一个特殊情形。从定义还可以看出，k 重传递群一定也是 $k-1$(如果 $k-1>0$)重传递群。一个置换群如果包含一个 k 重传递的子群，那么这个群也一定是 k 重传递的。如果 G 是一个传递群，但不是 2 重传递的，则称 G 是一个**单传递群**。

例1 由轮换(1,2,3,4,5,6)生成的 6 元置换群

$\{e,(1,2,3,4,5,6),(1,3,5)(2,4,6),(1,4)(2,5)(3,6),(1,5,3)(2,6,4),(1,6,5,4,3,2)\}$

是一个传递群，但不是 2 重传递的，所以是一个单传递群。

例2 5 元置换群

$\{e,(1,2,3,4,5),(1,3,5,2,4),(1,4,2,5,3),(1,5,4,3,2),(2,3,5,4),(1,3,2,5),(1,5,3,4),(1,2,4,3),(1,4,5,2),(2,4,5,3),(1,4,3,5),(1,2,5,4),(1,5,2,3),(1,3,4,2),(2,5)(3,4),(1,5)(2,4),(1,4)(2,3),(1,3)(4,5),(1,2)(3,5)\}$

是一个双传递群。证明留给读者。

因为 S_n 包含全部 n 元置换，所以 S_n 是 n 重传递群。下述例子给出 A_n 的传递重数。

例3 A_n $(n\geqslant 3)$是 $n-2$ 重传递的。

证明 对于任意 $n-2$ 个点 $a_{i_1},a_{i_2},\cdots,a_{i_{n-2}}$，总可适当选取 $a_{i_{n-1}},a_{i_n}$ 的次序使

$$g=\begin{pmatrix}a_1 & a_2 & \cdots & a_{n-2} & a_{n-1} & a_n\\ a_{i_1} & a_{i_2} & \cdots & a_{i_{n-2}} & a_{i_{n-1}} & a_{i_n}\end{pmatrix}$$

是一个偶置换。因此 $g\in A_{n-2}$，A_{n-2} 是 $n-2$ 重传递群。

从定义直接判断一个置换群是否为 k 重传递的是很麻烦的。下面来给出一个较为简单的方法。

定理6 设 G 是 $\Omega=(a_1,a_2,\cdots,a_n)$ 上的一个传递群。G 是 $k(k\geqslant 2)$重传递群的一个必要充分条件是 G_{a_1} 作为 $n-1$个

点$\{a_2,\cdots,a_n\}$上的置换群是$k-1$重传递的。

证明 设G是k重传递的。在$\{a_2,\cdots,a_n\}$中任取$k-1$个点$a_{i_2},a_{i_3},\cdots,a_{i_k}$，由$G$的$k$重传递性，在$G$中有一个置换$g$使得

$$a_1^g=a_1,a_2^g=a_{i_2},\cdots,a_k^g=a_{i_k}.$$

$g\in G_{a_1}$并把$a_2,\cdots,a_k$依次映到$a_{i_2},\cdots,a_{i_k}$。所以G_{a_1}是$k-1$重传递的。

设G_{a_1}是$k-1$重传递的。任取Ω中k个点$a_{i_1},a_{i_2},\cdots,a_{i_k}$，因为$G$是传递的，故有$g\in G$使$a_{i_1}^g=a_1$。设

$$g=\begin{pmatrix}a_{i_1} & a_{i_2} & \cdots & a_{i_k} & \cdots\\ a_1 & a_{j_2} & \cdots & a_{j_k} & \cdots\end{pmatrix}.$$

由G_{a_1}的$k-1$重传递性，存在$h\in G_{a_1}$使

$$a_{i_2}^h=a_{j_2},a_{i_3}^h=a_{j_3},\cdots,a_{i_k}^h=a_{j_k}.$$

于是

$$gh=\begin{pmatrix}a_{i_1} & a_{i_2} & \cdots & a_{i_k} & \cdots\\ a_1 & a_2 & \cdots & a_k & \cdots\end{pmatrix},$$

$$(gh)^{-1}=\begin{pmatrix}a_1 & a_2 & \cdots & a_k & \cdots\\ a_{i_1} & a_{i_2} & \cdots & a_{i_k} & \cdots\end{pmatrix}.$$

所以G是k重传递的。▎

从定理6的证明可看出，如果把a_1换成另一个点a_i，结论仍然成立。因此有下述推论。

推论1 设G是n元传递群。如果G_{a_1}是$n-1$元$k-1$重传递群，那么G_{a_i} $(i=2,3,\cdots,n)$也都是$n-1$元$k-1$重传递群。

证明 如果G_{a_1}是$n-1$元$k-1$重传递群，那么G是n元k重传递群。因此G_{a_i} $(i=2,\cdots,n)$是$n-1$元$k-1$重传递群。▎

反复应用定理6，还可得下述结论

推论2 如果G是n元k重传递群，那么G的保持$r(r<k)$个点的稳定子群是$n-r$元$k-r$重传递群。而G的保持k个点的稳定子群是一个$n-k$元非传递群。

定理6不仅可以用来推断传递群的传递重数，还可以用来讨论多重传递群的阶。

定理7 如果G是n元k重传递群，那么G的阶是

$$P_n^k=n(n-1)\cdots(n-k+1)$$

的一个倍数。

证明 反复应用定理4及定理6，即得

$$|G|=n|G_{a_1}|=n(n-1)\ |G_{a_1a_2}|=\cdots$$

$$=n(n-1)\cdots(n-k+1)|G_{a_1,\cdots,a_k}|.\ ▎$$

设G是一个n元置换群。如果G是n重或$n-1$重传递的，那么G的阶一定是

$$n(n-1)\cdots2=n!$$

的倍数。所以G一定是n元对称群S_n。

如果G是一个n元$n-2$重传递群，那么G的阶一定是

$$n(n-1)\cdots3=n!/2$$

的倍数。所以G是n元对称群S_n或n元交错群A_n。

我们也知道S_n确实是n重传递群，A_n确实是$n-2$重传递群，所以，S_n是唯一的n元n重传递置换群；A_n是唯一的n元$n-2$重(非$n-1$重)传递置换群。

有很多非平凡的(即不等于S_n或A_n的)双传递群和3重

传递群。但是已知的4重传递群只有四个，就是Mathieu群$M_{11},M_{12},M_{23},M_{24}$。它们的次数分别是11,12,23,24，是法国数学家Emile Mathieu在1861年发现的。其中M_{12}和M_{24}是5重传递的，这是仅有的两个已知的5重传递群。而且M_{11}是M_{12}的稳定子群；M_{23}是M_{24}的稳定子群。这四个群都是单群。已经证明没有传递重数大于或等于6的传递置换群，而交错群$A_n(n\geqslant 6)$与这四个Mathieu群是仅有的4重传递的单置换群。

M_{23}的稳定子群是Mathieu群M_{22}，这也是一个单群。五个Mathieu群是最早发现的不属于有限单群的无穷系列的五个零散单群。顺便提一下，已经证明共有26个零散单群。

五个Mathieu群的阶是：

$$|M_{11}|=8\cdot 9\cdot 10\cdot 11,$$
$$|M_{12}|=8\cdot 9\cdot 10\cdot 11\cdot 12,$$
$$|M_{22}|=48\cdot 20\cdot 21\cdot 22,$$
$$|M_{23}|=48\cdot 20\cdot 21\cdot 22\cdot 23,$$
$$|M_{24}|=48\cdot 20\cdot 21\cdot 22\cdot 23\cdot 24.$$

§3 非传递群

设G是作用在$\Omega=\{a_1,a_2,\cdots,a_n\}$上的非传递群。那么$a_1^G=\Omega_1$是$\Omega$的一个真子集。在$\Omega$中取$a_k\overline{\in}\Omega_1$，令$\Omega_2=a_k^G$。那么必有

$$\Omega_1\cap\Omega_2=\varnothing.$$

如果$\Omega_1\cup\Omega_2\neq\Omega$，那么还可在$\Omega$中找一个既不属于$\Omega_1$也不属于$\Omega_2$的点$a_l$。令$\Omega_3=a_l^G$。那么$\Omega_1,\Omega_2,\Omega_3$是$\Omega$的两两不相交的非空子集。这样继续下去，就可把$\Omega$分成一些不相交的子集$\Omega_1,\Omega_2,\cdots,\Omega_s$，使得$\Omega$中每个点恰属于一个$\Omega_i$（$1\leqslant i\leqslant s$），而且每个$\Omega_i$中的点都可以用$G$中的置换互变，而不同的$\Omega_i$中的点不能用$G$中的置换互变。这些$\Omega_i$称做$G$的传递集。更一般地，我们有下述定义

定义3 设G是Ω上的一个置换群，Ω_1是Ω的一个子集。如果$\Omega_1^G=\Omega_1$，则称Ω_1是G的一个**不变区**。如果Ω_1是G的一个不变区，而且Ω_1中任意两个点都可以用G中的置换互变，就称Ω_1是G的一个**传递集**或**轨道**。

如果G是Ω上的置换群，那么对任一$a\in\Omega$，a^G就是G的一个传递集，而且，G的每个传递集都可这样得到。

从定义立即可知：G是传递群的充分必要条件是G只有一个传递集，即Ω。

由定理1可知G的传递集的长度是G的阶的因子。

如果Ω_1是G的一个传递集，那么对任一$g\in G$都有$\Omega_1^g=\Omega_1$。因此

$$g_1^{-1}G_{\Omega_1}g=G_{\Omega_1}g=G_{\Omega_1},\quad \forall g\in G.$$

所以G_{Ω_1}是G的一个正规子群。

例4 §1例1中的置换群G共有两个传递集：

$$\Omega_1=\{a_1,a_2,a_3\}及\ \Omega_2=\{a_4,a_5\}.$$
$$G_{\Omega_1}=\{e,(a_4,a_5)\}\lhd G,$$
$$G_{\Omega_2}=G_{a_4}\lhd G.$$

设G是Ω上一个非传递群，取定G的一个不变区Ω_1。设

$$\Omega_1=\{a_1,a_2,\cdots,a_k\}\ (k<n),$$

把Ω中其它文字记成$\beta_1,\beta_2,\cdots,\beta_l$ ($l+k=n$)。那么G中每个置换都可以表成

$$g=\begin{pmatrix}a_1 & a_2 & \cdots & a_k & \beta_1 & \beta_2 & \cdots & \beta_l\\ a_{i_1} & a_{i_2} & \cdots & a_{i_k} & \beta_{j_1} & \beta_{j_2} & \cdots & \beta_{j_l}\end{pmatrix}$$

$$=\begin{pmatrix}a_1 & a_2 & \cdots & a_k\\ a_{i_1} & a_{i_2} & \cdots & a_{i_k}\end{pmatrix}\begin{pmatrix}\beta_1 & \beta_2 & \cdots & \beta_l\\ \beta_{j_1} & \beta_{j_2} & \cdots & \beta_{j_l}\end{pmatrix}$$

$$=\begin{pmatrix}\beta_1 & \beta_2 & \cdots & \beta_l\\ \beta_{j_1} & \beta_{j_2} & \cdots & \beta_{j_l}\end{pmatrix}\begin{pmatrix}a_1 & a_2 & \cdots & a_k\\ a_{i_1} & a_{i_2} & \cdots & a_{i_k}\end{pmatrix}.$$

令

$$g_1=\begin{pmatrix}a_1 & a_2 & \cdots & a_k\\ a_{i_1} & a_{i_2} & \cdots & a_{i_k}\end{pmatrix},\quad g_2=\begin{pmatrix}\beta_1 & \beta_2 & \cdots & \beta_l\\ \beta_{j_1} & \beta_{j_2} & \cdots & \beta_{j_l}\end{pmatrix}.$$

那么 g_1是 Ω_1 上的一个置换，其作用与 g 在 Ω_1 上 的 作 用一样。g_2 是 $\Omega\backslash\Omega_1$ 上的置换，其作用与 g 在 $\Omega\backslash\Omega_1$ 上的 作用一样。g_1,g_2 由 g 唯一确定而且 g_1 与 g_2是可交换的:

$$g=g_1g_2=g_2g_1.$$

g_1 称为**由 g 诱导出的Ω_1 上的置换**。用 G^{Ω_1} 表示 G 中全部置换诱导出的 Ω_1 上的置换所成的集合。我们来证明:

定理8 设 Ω_1 是 G 的一个不变区，则

1）G^{Ω_1} 是 Ω_1 上的置换群。如果 Ω_1 是一个传 递 集，则 G^{Ω_1} 在 Ω_1 上是传递的。

2）G^{Ω_1} 是 G 的一个同态象，$G^{\Omega_1}\cong G/G_{\Omega_1}$。

证明 1）如果 $g_1,h_1\in G^{\Omega_1}$，那么有 $g,h\in G$，使

$$g=g_1g_2,\quad h=h_1h_2,$$

其中 g_2,h_2 都是作用于 $\beta_1,\beta_2,\cdots,\beta_l$ 上的置换。于是

$$gh=(g_1g_2)(h_1h_2)=(g_1h_1)(g_2h_2).$$

式中 g_1h_1 是 Ω_1 上的置换，g_2h_2 是 $\Omega\backslash\Omega_1$ 上的置换。因此，g_1h_1 是 gh 诱导出的 Ω_1 上的置 换，$g_1h_1\in G^{\Omega_1}$。所 以 G^{Ω_1}是一个群。

如果再设 Ω_1 是 G 的传递集，那么对Ω_1 中任意两个文字 a_i,a_j，有 $g\in G$，使

$$a_i^g=a_j.$$

所以 G^{Ω_1}在 Ω_1上是传递的。

2）作 G 到 G^{Ω_1} 上的映射

$$\varphi: g\mapsto g_1.$$

这个映射是映上的而且是保持运算的，所以是一个满同态，因此 G^{Ω_1}是 G 的一个同态象。

如果 $g^\varphi=g_1$ 是恒等置换，那么 g 一定把 Ω_1中每个点都保持不变，故 $g\in G_{\Omega_1}$。当然，当 $g\in G_{\Omega_1}$ 时，g 所 诱 导 出 的 Ω_1 上的置换一定是恒等置换，$g\in G_{\Omega_1}$。 所 以 φ 的 核 是 G_{Ω_1}，$G/G_{\Omega_1}\cong G^{\Omega_1}$。 ▌

定义4 G^{Ω_1} 称为 G 在 Ω_1 上的**成分**。如果 Ω_1 是 G 的 一 个传递集，则称 G^{Ω} 为 G 的一个**传递成分**。

从 G 的每个传递集都可以得到 G 的一 个 传 递 成分。因此，如果 G 有 s 个传递集，那么 G就有 s 个传递成分，因而得到 G 的 s 个传递的同态象。

例5 例4中的 G 有两个传递集

$$\Omega_1=\{a_1,a_2,a_3\},\quad \Omega_2=\{a_4,a_5\}.$$

所以 G 有两个传递成分:

$$G^{\Omega_1}=\{e,(a_1,a_2),(a_1,a_3),(a_2,a_3),(a_1,a_2,a_3),(a_1,a_3,a_2)\}\cong G/G_{\Omega_1},$$

$$G^{\Omega_2}=\{e,(a_4,a_5)\}\cong G/G_{\Omega_2}.$$

例6 $G=\{e,(a_1,a_2)(a_3,a_4),(a_5,a_6),$
$(a_1,a_2)(a_3,a_4)(a_5,a_6),(a_1,a_3)(a_2,a_4)(a_7,a_8),$

$$(a_1,a_3)(a_2,a_4)(a_5,a_6)(a_7,a_8),$$
$$(a_1,a_4)(a_2,a_3)(a_7,a_8),$$
$$(a_1,a_4)(a_2,a_3)(a_5,a_6)(a_7,a_8)\}$$

是一个 8 元非传递群，有三个传递集：

$$\Omega_1=\{a_1,a_2,a_3,a_4\},\quad \Omega_2=\{a_5,a_6\},\quad \Omega_3=\{a_7,a_8\}.$$

相应的传递成分为：

$$G^{\Omega_1}=\{e,(a_1,a_2)(a_3,a_4),(a_1,a_3)(a_2,a_4),(a_1,a_4)(a_2,a_3)\},$$
$$G^{\Omega_2}=\{e,(a_5,a_6)\},$$
$$G^{\Omega_3}=\{e,(a_7,a_8)\}.$$

保持 Ω_i 不动的正规子群是：

$$G_{\Omega_1}=\{e,(a_5,a_6)\},$$
$$G_{\Omega_2}=\{e,(a_1,a_2)(a_3,a_4),(a_1,a_3)(a_2,a_4)(a_7,a_8),$$
$$(a_1,a_4)(a_2,a_3)(a_7,a_8)\},$$
$$G_{\Omega_3}=\{e,(a_1,a_2)(a_3,a_4),(a_5,a_6),(a_1,a_2)(a_3,a_4)(a_5,a_6)\}.$$

容易验证

$$G/G_{\Omega_i}\cong G^{\Omega_i},\quad i=1,2,3.$$

因为非传递置换群 G 的传递成分是 G 的传递的同态象，因此可以通过传递群来研究和构造非传递置换群。

§4 传递群作为群的置换表示

4.1 置换同构

以前我们讨论了群的正则表示及陪集置换表示，这样就可以利用置换群来讨论一般群。这一节来证明，我们总可以把传递群看成某个群的正则表示或陪集表示，因而使我们可以应用群群的传递置换表示的性质来讨论传递群。

为了确切地理解这个问题，需要引入置换同构的概念。

定义5 设 G 是 Ω 上的一个置换群，G' 是 Ω' 上的一个置换群。如果存在 Ω 到 Ω' 上的一个一一对应 σ，以及 G 到 G' 的一个一一对应 φ，使得对任一 $a\in\Omega$ 都有

$$(a^g)^\sigma=(a^\sigma)^{g^\varphi}.$$

则称 G 与 G' 是**置换同构的**，记作 $G\cong_p G'$。

如果 G 与 G' 是满足定义中条件的一对置换同构的群，设

$$\Omega=\{a_1,a_2,\cdots,a_n\}.$$

则
$$\Omega'=\{a_1^\sigma,a_2^\sigma,\cdots,a_n^\sigma\}.$$

如果 g 是 G 中任一个元素，

$$g=\begin{pmatrix}a_i\\a_{j_i}\end{pmatrix},$$

g 在映射 φ 下所对应的置换为 g^φ，

$$g^\varphi=\begin{pmatrix}a_i^\sigma\\(a_i)^{g^\varphi}\end{pmatrix}=\begin{pmatrix}a_i^\sigma\\(a_i^g)^\sigma\end{pmatrix}.$$

这就是说，在 g 中把每个 a_i 换成 a_i 在 σ 下的象 a_i^σ 就得到 g^φ。因此 g 与 g^φ 只是所作用的点的表法不一样，而它们的作用是相同的。因而 G 与 G' 作为置换群可以看成是相同的。

可以证明，定义 5 中的一一对应 φ 一定是 G 到 G' 的一个同构映射。这是因为对于 G 中任意两个元素 g_1,g_2，任取 Ω 中一个点 a，从定义可知

$$\begin{aligned}(a^\sigma)^{g_1^\varphi g_2^\varphi}&=((a^\sigma)^{g_1^\varphi})^{g_2^\varphi}=((a^{g_1})^\sigma)^{g_2^\varphi}\\&=((a^{g_1})^{g_2})^\sigma=(a^{g_1g_2})^\sigma\\&=(a^\sigma)^{(g_1g_2)^\varphi}.\end{aligned}$$

其中 a^σ 可以是 Ω' 中任一个点。因此有

$$(g_1g_2)^\varphi = g_1^\varphi g_2^\varphi.$$

又因 φ 是一一的，所以 φ 是一个同构映射。

因此，置换同构的群一定是同构的。但是同构的群不一定是置换同构的。例如，设

$$G = \{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\},$$

$$G' = \{e,(1,2),(3,4),(1,2)(3,4)\}.$$

那么，G 与 G' 作为抽象群是同构的，但是它们不是置换同构的。不仅如此，G 在$\{1,2,3,4\}$上是传递的，而 G' 是非传递的。因此它们作为置换群是有很大差别的。这说明同构(而非置换同构)的群不一定有相同的传递性。这一点在讨论置换群时是需要注意的。

4.2　一般传递群作为陪集置换表示

定理9　任一传递置换同构于某个群的陪集置换表示。

证明　设 G 是 n 元集合

$$\Omega = \{a_1,a_2,\cdots,a_n\}$$

上的一个传递置换群。再设 $H = G_{a_1}$是 G 对 a_1的稳定子群。于是

$$G = Hg_1 \cup Hg_2 \cup \cdots \cup Hg_n, \quad Hg_1 = H.$$

式中的置换g_i满足

$$a_1^{g_i} = a_i \qquad (i = 1,2,\cdots,n).$$

下面来证 G 对 H 的陪集置换表示 $S_{G/H}$ 与 G 是置换同构的。

任取 G 中一个置换 g，设

$$g = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_{j_1} & a_{j_2} & \cdots & a_{j_n} \end{pmatrix}.$$

g 所对应的陪集置换为

$$\omega_g = \begin{pmatrix} Hg_1 & Hg_2 & \cdots & Hg_n \\ Hg_1g & Hg_2g & \cdots & Hg_ng \end{pmatrix}.$$

Hg_ig等于哪个陪集取决于a_1 在g_ig下的象。由于

$$a_1^{g_ig} = a_i^g = a_{j_i},$$

所以　　$Hg_ig = Hg_{j_i} \qquad (i = 1,2,\cdots,n),$

$$\omega_g = \begin{pmatrix} Hg_1 & Hg_2 & \cdots & Hg_n \\ Hg_{j_1} & Hg_{j_2} & \cdots & Hg_{j_n} \end{pmatrix}.$$

用 φ 表示 G 到 $S_{G/H}$上的映射：

$$g^\varphi \mapsto \omega_g,$$

那么，由于

$$\bigcap_{g\in G} g^{-1}G_{a_1}g = \bigcap_i G_{a_i} = \{e\},$$

所以 φ 是 G 到 $S_{G/H}$ 的一个同构映射。再定义Ω到

$$\Omega' = \{Hg_1,Hg_2,\cdots,Hg_n\}$$

的映射 σ 为

$$a_i^\sigma \mapsto Hg_i, \qquad i = 1,2,\cdots,n.$$

那么σ是一一对应，并且

$$(a_i^g)^\sigma = (a_{i_j})^\sigma = Hg_{i_j} = (Hg_i)^{\omega_g}$$

$$= (a_i^\sigma)^{\omega_g} = (a_i^\sigma)^{g^\varphi}.$$

所以G 与$S_{G/H}$是置换同构的。▍

因此，任一传递置换群都可看作是某个群的陪集置换表示。

4.3　正则置换群作为正则表示

定义 6　G 是 Ω上的一个置换群，如果G 对于 Ω中任一

个点 a 的稳定子群都是单位子群，则称 G 是**半正则群**。传递的半正则群称为**正则群**。

从定义可知，正则群一定是半正则的。半正则群的子群及成分也都是半正则的。

我们知道，一个群的正则表示一定是正则群。反之，我们有

定理10 任一正则群都与某个群的正则表示置换同构。

证明 设 G 是一个正则群，那么 G 的稳定子群为单位子群 E，而 G 对 E 的陪集置换表示就是 G 的右正则表示。因此从定理 9 的证明可知 G 与其右正则表示是置换同构的。▍

正则群是一类重要的置换群。下面介绍正则群的一些重要性质。

设 G 是 Ω 上的一个正则群，$\alpha\in\Omega$。从关于稳定子群的阶的重要公式

$$|G|=|G_\alpha||\alpha^G|$$

可推知正则群的传递集都有相同的长度，即 $|G|$。因此，我们有下述定理。

定理11 n 元半正则群的阶一定是 n 的一个因数。一个 n 元传递群是正则群的充分必要条件是它的阶等于 n。

我们来给出另一类正则群。

定理12 设 G 是 Ω 上一个交换的传递群，S 是 Ω 上的对称群。则

1） G 是一个正则群。

2） G 在 S 内的中心化子就等于 G。

证明 1）因为 G 是传递的，所以对于 Ω 中任意两个文字 α,β，存在 G 中一个置换 g 使得 $\alpha^g=\beta$。又因 G 是交换的。所以

$$G_\alpha=g^{-1}G_\alpha g=G_{\alpha^g}=G_\beta.$$

因为 α,β 可以是 Ω 中任意的文字，所以 $G_\alpha=\{e\}$，G 是半正则的。再因 G 是交换群，所以 G 是正则的。

2）用 Z 表示 G 在 S 内的中心化子。因为 G 是交换的，所以 $G\leqslant Z$，因之 Z 是传递的。设 α,β,g 如上，则

$$Z_\alpha=g^{-1}Z_\alpha g=Z_\alpha g=Z_\beta.$$

所以 $Z_\alpha=\{e\}$，Z 是正则的。比较 Z 与 G 的阶，即得 $G=Z$。▍

§5 本 原 性

5.1 定 义

定义 7 G 是 Ω 上的一个传递群。如果 Ω 可以分成一些不相交的子集

$$\Omega=\Pi_1\cup\Pi_2\cup\cdots\cup\Pi_s\quad(1<s<n),\ \Pi_i\cap\Pi_j=\varnothing(i\neq j),$$

使得 G 中每个置换将每个 Π_i $(i=1,2,\cdots,s)$ 仍变为某个 Π_j，那么 G 就称为一个**非本原群**。Π_i $(i=1,2,\cdots,s)$ 称为 G 的**非本原集**。$\Pi_1,\Pi_2,\cdots,\Pi_s$ 称为 G 的一个**非本原系**。如果 G 不是非本原群，则称 G 为**本原群**。

例 1 由 (a_1,a_2,a_3,a_4,a_5) 生成的 5 元 5 阶传递置换群 G 是一个本原群。

例 2 G 是 S_6 的一个子群，它由下列两个置换生成

$$g=(1,2,3,4,5,6),\qquad h=(2,6)(3,5).$$

因为
$$hg=g^5h,$$
所以 G 中共有12个元素：

$$g^lh^m,\quad l=0,1,2,\cdots,5,\quad m=0,1.$$

很容易看出 G 是传递的。将 $\Omega=\{1,2,3,4,5,6\}$ 分成三个不相交的子集

$$\Omega=\{1,4\}\cup\{2,5\}\cup\{3,6\}.$$

那么，因为

$$\{1,4\}\overset{g}{\mapsto}\{2,5\},\ \{1,4\}\overset{h}{\mapsto}\{1,4\},$$
$$\{2,5\}\overset{g}{\mapsto}\{3,6\},\ \{2,5\}\overset{h}{\mapsto}\{3,6\},$$
$$\{3,6\}\overset{g}{\mapsto}\{1,4\},\ \{3,6\}\overset{h}{\mapsto}\{2,5\},$$

所以G是一个本原群。$\{1,4\},\{2,5\},\{3,6\}$是G的三个非本原集，构成G的一个非本原系。

还可以将Ω分成两个非本原集

$$\Omega=\{1,3,5\}\cup\{2,4,6\}.$$

$\{1,3,5\}$，$\{2,4,6\}$也是G的一个非本原系。

上面的例子说明一个非本原群的非本原系不是唯一的。但是我们有下述定理。

定理13 G是一个非本原群，$\Pi_1,\Pi_2,\cdots,\Pi_s$是一个非本原系，那么Π_i $(i=1,2,\cdots,s)$的长度都相等。

证明 任取$a_i\in\Pi_i$，$a_j\in\Pi_j$。因为G是传递的，所以有一个置换$g\in G$将a_i映到a_j。于是

$$a_j\in\Pi_i^g\cap\Pi_j,\ \Pi_i^g\cap\Pi_j\neq\varnothing.$$

由非本集的定义，得

$$\Pi_i^g=\Pi_j.$$

因此$|\Pi_i|=|\Pi_j|$。 ▌

推论1 n元非本原群的非本原集的长度是n的因子，其非本原系中非本原集的个数也是n的因子。

推论2 对于任意素数p，p元传递群一定是本原的。

从本原群的定义可以证明多重传递群一定是本原的，证明留给读者作为习题(本章习题18)。

5.2 判别定理

首先来讨论陪集置换表示的本原性。

设G是一个n阶群，H是G的一个真子群。如果G没有一个异于H的真子群能包含H，则称H为G的一个**极大子群**。因此，如果H是G的一个极大子群，那么从

$$G\geqslant K\geqslant H$$

可推出$K=G$或H。如果H不是G的极大子群，那么可找到G的一个子群K使

$$G>K>H.$$

当$G\geqslant K\geqslant H$时，G对K,G对H,K对H的指数及陪集代表的关系，我们已在第一章§5定理9中讨论过。

定理14 G对子群H的陪集置换表示$S_{G/H}$是本原群的充分必要条件是：H是G的一个极大子群。

证明 设$S_{G/H}$是非本原的，并设

$$\{H=Hg_1,Hg_2,\cdots,Hg_l\}$$

是包含H的一个非本原集。令

$$K=Hg_1\cup Hg_2\cup\cdots\cup Hg_l.$$

下面来证K是G的一个子群。

任取K中两个元素$hg_i,h'g_j$ $(h,h'\in H,1\leqslant i,j\leqslant l)$。考虑$hg_i$对应的陪集置换：

$$\omega_{hg_i}=\begin{pmatrix}H & Hg_2 & \cdots & Hg_l\\ Hhg_i & Hg_2hg_i & \cdots & Hg_lhg_i\end{pmatrix}$$

$$=\begin{pmatrix}H & Hg_2 & \cdots & Hg_l\\ Hg_i & Hg_2hg_i & \cdots & Hg_lgh_i\end{pmatrix}.$$

因为$\{Hg_1,Hg_2,\cdots,Hg_l\}$是一个非本原集，而且$H$在$\omega_{hg_i}$下

的象仍在这个集合中，所以由非本原集的定义，

$$\{Hg_i,Hg_2g_i,\cdots,Hg_lg_i\}=\{Hg_1,Hg_2,\cdots,Hg_l\}.$$

设 $$Hg_jhg_i=Hg_t,\ 1\leqslant t\leqslant l\ .$$

则 $$h'g_jhg_i=h''g_t\in K.$$

所以K是G的一个子群。因为$S_{G/H}$的非本原集是$S_{G/H}$作用的集合

$$\{H,Hg_2,\cdots,Hg_r\}(r=G/H)$$

的非平凡真子集，故有$1<l<r$。所以$G>K>H$。H不是G的极大子群。

另一方面，如果H不是极大子群，则有G的子群K满足

$$G>K>H.$$

设G对K,K对H的陪集分解为：

$$G=Kg_1\cup Kg_2\cup\cdots\cup Kg_l,$$
$$K=Hh_1\cup Hh_2\cup\cdots\cup Hh_m.$$

则G对H的陪集分解为

$$G=\bigcup_{i,j}Hh_ig_j.$$

我们来证

$$\Pi_1=\{Hh_1g_1,Hh_2g_1,\cdots,Hh_mg_1\},$$
$$\Pi_2=\{Hh_1g_2,Hh_2g_2,\cdots,Hh_mg_2\},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\Pi_l=\{Hh_1g_l,Hh_2g_l,\cdots,Hh_mg_l\}$$

是$S_{G/H}$的一个非本原系。

任取$g\in G$，设g所对应的陪集置换为ω_g。考虑

$$\Pi_i=\{Hh_1g_i,Hh_2g_i,\cdots,Hh_mg_i\}$$

在置换ω_g下的象

$$\Pi_i^{\omega_g}=\{Hh_1g_ig,Hh_2g_ig,\cdots,Hh_mg_ig\}.$$

因为 $$\bigcup_{t=1}^{m}Hh_tg_i=Kg_i$$

是K的一个陪集，所以

$$\bigcup_{t=1}^{m}Hh_tg_ig=(\bigcup Hh_tg_i)g=Kg_ig$$

也是K的一个陪集。

设 $$Kg_ig=Kg_j.$$

则$Hh_1g_ig,Hh_2g_ig,\cdots,Hh_mg_ig$就是

$$Hh_1g_j,Hh_2g_j,\cdots,Hh_mg_j$$

的一个排列。因此

$$\Pi_i^{\omega_g}=\Pi_j.$$

这就证明了$\Pi_1,\Pi_2,\cdots,\Pi_s$是G的一个非本原系，G是非本原的。 ▎

例 3 第一章§7例4中的H是G的极大子群，所以这个陪集置换表示是非本原的。而例5中的H不是极大子群。所以相应的陪集置换表示是非本原的。$\{H,Ha\}$与$\{H,Hab\}$是$S_{G/H}$的一个非本原系。

因为传递群G可看成G对G_{a_1}的陪集置换表示，所以我们可以应用上述定理得到关于置换群的本原性的一个判别法则。

定理15 G是Ω上一个传递群。G是本原群的充分必要条件是G的稳定子群G_α $(\alpha\in\Omega)$是G的一个极大子群。

从定理15可以得到下面一些推论。

推论 1 G是Ω上一个传递群。如果G_α $(\alpha\in\Omega)$还保持Ω中另一个点β不变，那么G或者是非本原的，或者是素数次正则群。

证明 如果G是正则群，则因$|G|$是复合数时，G一定有非平凡子群。故如果$|G|$不是素数，那么G一定是非本原的。

设G是非正则的，即$G_a \neq \{1\}$，并设G_a一共有t个不动点。那么$1<t<n$。由定理5，G_a有t个共轭子群，因此

$$|G:N_G(G_a)| = n/t > 1.$$

又因$|G:G_a| = n > \frac{n}{t}$，所以

$$G > N_G(G_a) > G_a.$$

G_a不是G的极大子群，G是非本原的。▎

推论 2 设G是Ω上一个传递群。如果Ω有一个眞子集Π，Π不止包含一个文字，而且

$$a \in \Pi, a^g \in \Pi \rightarrow \Pi^g = \Pi,$$

那么G是非本原的。

证明 取定$a \in \Pi$，只要证明G_a不是G的极大子群。为此考虑G的子群$G_{\{\Pi\}}$。我们来证$G_{\{\Pi\}}$是G与G_a的中间群。

由假设，知$G_{\{\Pi\}} \geqslant G_a$。但是由$G$的传递性，对于$\beta \in \Pi$，$\beta \neq a$一定有一个$g \in G$使$a^g = \beta$。这个置换$g \in G_{\{\Pi\}}$但不属于$G_a$，所以$G_{\{\Pi\}} > G_a$。

再取$\gamma \overline{\in} \Pi$，由$G$的传递性，存在$g' \in G$使$a^{g'} = \gamma$，于是

$$g' \overline{\in} G_{\{\Pi\}}，\ G_{\{\Pi\}} < G.$$

因此G_a不是G的极大子群，G是非本原的。▎

这个推论给出了一个求非本原系的方法。推论中的Π就是一个非本原集。因为由假设可知对任一$g \in G$，有

$$\Pi^g \cap \Pi = \Pi \text{或} \varnothing.$$

故由G的传递性可将Ω表成不相交的子集之并

$$\Omega = \Pi \cup \Pi^{g_2} \cup \cdots \cup \Pi^{g_s}.$$

于是$\Pi, \Pi^{g_2}, \cdots, \Pi^{g_s}$就是$G$的一个非本原系。

定理16 如果Ω上传递群G有一个非传递正规子群$N \neq \{e\}$，那么G是非本原的，而且N的传递集是G的一个非本原集。

证明 任取N的一个传递集

$$\Pi = \{a_1, a_2, \cdots, a_m\}, \quad 1 < |\Pi| < |\Omega|.$$

来证Π满足定理15推论 2 中的条件。

设G中置换g把Π中一个点a_i仍映到Π中：

$$a_i^g \in \Pi.$$

为了证明$\Pi^g = \Pi$，只要证明对Π中任一个点a_j，都有$a_j^g \in \Pi$。因为Π是N的传递集，故有$h \in N$使$a_i^h = a_j$。于是

$$a_j^g = a_i^{hg} = (a_i^g)^{g^{-1}hg} \in \Pi^{g^{-1}hg}.$$

因为N是G的正规子群，所以$g^{-1}hg \in N$。故$\Pi^{g^{-1}hg} = \Pi$。$a_j^g \in \Pi$。▎

推论 本原群的非单位正规子群一定是传递的。

5.3 非本原系置换群

设G是一个非本原群。如果$\Pi_1, \Pi_2, \cdots, \Pi_s$是$G$的一个非本原系，那么$G$中一个元素$g$引起$\Pi_1, \Pi_2, \cdots, \Pi_s$的一个置换

$$\theta_g = \begin{pmatrix} \Pi_1 & \Pi_2 & \cdots & \Pi_s \\ \Pi_1^g & \Pi_2^g & \cdots & \Pi_s^g \end{pmatrix} = \begin{pmatrix} \Pi_i \\ \Pi_i^g \end{pmatrix}.$$

令

$$P = \{\theta_g \mid g \in G\}.$$

P是一个s次置换群，称为G的一个非本原系置换群。

映射$g \mapsto \theta_g$是G到P的一个满同态，这个同态映射的核是由G中满足

$$\Pi_i^g = \Pi_i, \quad i=1,2,\cdots,s$$

的置换所组成。于是根据同态定理，有

定理17 设G是一个非本原群，$\Pi_1,\Pi_2,\cdots,\Pi_s$是G的一个非本原系，P是G的对应于$\Pi_1,\Pi_2,\cdots,\Pi_s$的非本原系置换群。令

$$K=\{g\in G \mid \Pi_i^g=\Pi_i, \quad i=1,2,\cdots,s\}.$$

那么K是G的一个正规子群，而且$P\cong G/K$。

P是一个传递群，它的次数比G的次数小得多。因为P是G的同态象，所以可以利用非本原系置换群来讨论非本原群。

非本原群G的非本原系置换群可能还是非本原的。下面来证明总可选择G的一个非本原系，使G对此非本原系的置换表示是本原的，从而可以通过本原群来讨论非本原群。

设G是一个非本原群，$\Pi_1,\Pi_2,\cdots,\Pi_s$是G的一个非本原系，P是G对$\Pi_1,\Pi_2,\cdots,\Pi_s$的非本原系置换群。如果P是一个非本原群。则$\{\Pi_1,\Pi_2,\cdots,\Pi_s\}$可以分成一些不相交的非本原集，设为

$$\{\Pi_{i1},\Pi_{i2},\cdots,\Pi_{it}\}, \quad i=1,2,\cdots,s/t, 1<t<s.$$

令

$$\Psi_i=\bigcup_j \Pi_{ij}, \quad i=1,2,\cdots,s/t.$$

下面来证$\Psi_1,\Psi_2,\cdots,\Psi_r (r=s/t)$也是$G$的一个非本原系。

首先有

$$\Omega=\bigcup_{1<i<r}\Psi_i, \quad \Psi_i\cap\Psi_j=\varnothing (i\neq j), 1<r<n.$$

任取$g\in G$，则

$$\Psi_i^g=\Big(\bigcup_{1<j<t}\Pi_{ij}\Big)^g=\bigcup_j(\Pi_{ij}^g).$$

因为$\{\Pi_{i1},\Pi_{i2},\cdots,\Pi_{it}\}, i=1,2,\cdots,r$是一个非本原系，所以可找到一个$j$使得

$$\{\Pi_{i1}^g,\Pi_{i2}^g,\cdots,\Pi_{it}^g\}=\{\Pi_{j1},\Pi_{j2},\cdots,\Pi_{jt}\} \quad (1\leqslant j\leqslant r).$$

于是
$$\Psi_i^g=\Psi_j.$$

这就证明了$\Psi_1,\Psi_2,\cdots,\Psi_r$也是$G$的一个非本原系。

考虑G对$\Psi_1,\Psi_2,\cdots,\Psi_r$的非本原系置换群$P_1$。如果$P_1$是非本原的，那么又可将$\Psi_i$合并成一些较大的非本原集。由于$\Omega$是一个有限集合，这个过程一定会在若干次之后终止。这样就得到G的一个非本原系，使G的对应的非本原系置换群是本原的。

置换群理论的重要问题之一是找出给定次数的全部互不置换同构的置换群。置换群论的早期工作有很多是有关构作低次置换群方面的问题。在第一章中我们曾经提到过，次数不超过11的置换群已经全部决定，当$12\leqslant n\leqslant 15$时，已决定了全部$n$次传递群。而当$n$较大时，仅对$16\leqslant n\leqslant 30$找出了全部$n$次本原群。

习　题

1．对第二章习题9中的置换群G，求G_{a_i} $(i=1,2,\cdots,7)$及其共轭子群。

2．令$\Gamma=\{\alpha_1,\alpha_2\}$。求上题中$G$的$G_\Gamma$及$G_{(\Gamma)}$，并验证$G_\Gamma\lhd G_{(\Gamma)}$。

3．(1) 设G是Ω上一个传递群，T是G的一个传递子

群。则对任一$a\in\Omega$，都有$G=TG_a$。

(2) 对$G=A_4$验证这一结论。

4. G是n次对称群S_n的一个子群，$\sigma\in S_n$。如果Δ是G的一个轨道，则Δ^σ是$\sigma^{-1}G\sigma$的一个轨道。

5. 设N是传递置换群G的一个正规子群，则N的轨道长度都相等。

6. G是S_n的一个传递子群，则$Z_{S_n}(G)$是半正则的。

7. (1) 如果G是$\Omega=\{a_1,a_2,\cdots,a_n\}$上一个2重传递群，则$G_{a_ia_j}$与$G_{a_ka_l}$共轭($i\neq j,k\neq l,1\leqslant i,j,k,l\leqslant n$)。

(2) 假设$G_{a_ia_j}$一共保持k个文字不变，问S_n有多少个与$G_{a_ia_j}$共轭的子群？

8. $G=\langle(1,3,6),(2,5,9),(4,7)\rangle<S_9$。求$G$的全部传递集，并对每个传递集$\Delta$求$G_\Delta$及$G^\Delta$。

9. 求第1题中置换群G的传递集及传递成分。

10. 设$G=\langle\sigma\rangle$。则σ的轮换表示中同一轮换中的点组成G的传递集。

11. 设Δ是置换群G的一个传递集，$a\in\Delta$。证明：G_a在G中的共轭子群的个数等于$(G^\Delta)_a$在G^Δ中的共轭子群的个数。

12. 如果G是一个传递群，那么G中每个置换平均有一个不动点，即G中各置换的不动点的总数等于$|G|$。

13. 如果G是一个非传递群，共有k个传递集，则G中每个置换平均有k个不动点。

14. 证明n次传递群中一定有n次置换。

15. 设G_1是$\Omega_1=\{a_1,a_2,\cdots,a_s\}$上一个置换群，$G_2$是$\Omega_2=\{\beta_1,\beta_2,\cdots,\beta_t\}$上一个置换群，$a_1,\cdots a_s,\beta_1,\cdots,\beta_t$各不相同。对$g_1\in G_1,g_2\in G_2$，$g_1g_2$可看成作用于

$$\Omega=\Omega_1\cup\Omega_2=\{a_1\cdots,a_s,\beta_1\cdots,\beta_t\}$$

上的一个置换。令

$$G=\{g_1g_2\,|\,g_1\in G_1,g_2\in G_2\}。$$

证明：

(1) G是Ω上的一个置换群。

(2) 如果G_1在Ω_1上传递，G_2在Ω_2上传递，则G以Ω_1及Ω_2作为传递集。

(3) G_1,G_2都是G的正规子群。

G称为G_1与G_2的直积，记作$G_1\otimes G_2$。

16. 设G是一个非传递群，有两个传递集Ω_1,Ω_2。证明：

(1) $G\leqslant G^{\Omega_1}\otimes G^{\Omega_2}$。

(2) $G=G^{\Omega_1}\otimes G^{\Omega_2}\Leftrightarrow G\geqslant G^{\Omega_i},i=1,2$。

17. 设G是由$(1,2,\cdots,n)$生成的循环群，看成S_n的子群。

(1) 证明G是本原群的充分必要条件是n是一个素数。

(2) 当n是复合数时，求G的非本原集。

18. 证明双传递群一定是本原的。

19. 对§5例2验证定理17。

20. 设G是pq次非本原群，p与q都是素数，证明G的非本原系置换群一定是本原的。

第四章　交　换　群

交换群是很重要也是很常见的一类群。因为任何一个群都可能有交换的子群及交换的商群，所以交换群的理论在整个群论中占有很重要的地位。

交换群的理论已经研究得相当好。这一章介绍交换群的构造理论。

§1　直　　积

为了将一个群用它的子群来表示，需要用到子群的直积的概念。这一节介绍子群的直积的一些性质。

定义 1　设 G 是一个群，A 与 B 是 G 的子群。如果

(1)　G 中每个元素 g 都可表成

$$g=ab,\quad a\in A,\quad b\in B.$$

而且表法是唯一的。

(2)　A 中元素与 B 中元素可交换。

那么称 G 为子群 A 与 B 的**直积**，记作 $G=A\otimes B$。A 与 B 称为 G 的**直积因子**。

当 G 是交换群的情形，直积称为**直和**，记作 $G=A\oplus B$。A 与 B 称为 G 的**直和因子**。

从直积的定义可以看出，如果 $G=A\otimes B$，那么有

1.　$G=B\otimes A$。

2.　$|G|=|A|\cdot|B|$。

3.　G 是交换群的充分必要条件是 A 与 B 都是交换群。

下面来对直积的定义作一点补充：定义中表法的唯一性只要对单位元素要求就够了。即从单位元素表法的唯一性可以推出任一元素表法的唯一性。可以这样来证明：如果

$$g=ab=a'b',\quad a,a'\in A;\quad b,b'\in B$$

是 G 中元素 g 的两种表法，那么

$$(a^{-1}a')(b'b^{-1})=e.$$

根据单位元素表法的唯一性，有

$$a^{-1}a'=b'b^{-1}=e.$$

即

$$a=a',\quad b=b'.$$

这就是我们所要证明的。

子群的直积有下述重要性质，这个性质也可以用来作为直积的定义。

定理 1　如果 $G=A\otimes B$，那么有

1.　A,B 都是 G 的正规子群。

2.　$G=AB$。

3.　$A\cap B=\{e\}$。

反之，如果 G 的子群 A,B 满足上述三个条件，那么 $G=A\otimes B$。

证明　设 $G=A\otimes B$，那么从定义立刻推出 $G=AB$。$A\cap B=\{e\}$ 可以从表法的唯一性推出：如果 $c\in A\cap B$，那么 c 可表成

$$c=c\cdot e,\quad c\in A,\quad e\in B.$$

又可表成

$$c=e\cdot c,\quad e\in A,\quad c\in B.$$

所以从表法的唯一性立刻得到

$$c=e.$$

即

$$A\cap B=\{e\}.$$

再来证A,B是G的正规子群。任取$a\in A,g\in G$，要证$g^{-1}ag\in A$。根据直积的定义，有$a_1\in A$，$b_1\in B$，使$g=a_1b_1$。于是

$$g^{-1}ag=(a_1b_1)^{-1}a(a_1b_1)=b_1^{-1}a_1^{-1}a\,a_1b_1$$
$$=a_1^{-1}aa_1b_1^{-1}b_1=a^{-1}aa_1\in A.$$

所以$A\triangleleft G$。同样可证$B\triangleleft G$。

现在假设G的子群A,B满足定理1中的三个条件，来证$G=A\otimes B$。

从$G=AB$可以推出对G中任一元素g，都有$a\in A$，$b\in B$使$g=ab$。下面来证表法是唯一的。如果

$$g=ab=a'b',\quad a,a'\in A;\quad b,b'\in B.$$

那么

$$a'^{-1}a=b'b^{-1}\in A\cap B.$$

由假设$A\cap B=\{e\}$，

所以 $$a'^{-1}a=b'b^{-1}=e.$$

即 $$a=a',\quad b=b'.$$

这就证明了表法的唯一性。

最后来证A中元素与B中元素可交换。任取$a\in A$，$b\in B$。因为A,B都是正规子群，所以有

$$aba^{-1}b^{-1}=a(ba^{-1}b)\in A$$

及

$$aba^{-1}b^{-1}=(aba^{-1})b^{-1}\in B.$$

从$A\cap B=\{e\}$，即得

$$aba^{-1}b^{-1}=e.$$

亦即

$$ab=ba.$$

定理证毕。 ▌

子群的直积可以推广到几个直积因子的情形。

定义 2 设$A_1,A_2,\cdots,A_s(s\geqslant 2)$都是$G$的子群。如果

(1) G中任一元素g都可以唯一地表成

$$g=a_1a_2\cdots a_s,\quad a_i\in A_i(i=1,2,\cdots,s).$$

(2) A_i中任意元素与A_j中任意元素可交换（$i,j=1,2,\cdots,s$；$i\neq j$）。那么G称为$A_1,A_2,\cdots,A_s$的直积，记作$G=A_1\otimes A_2\otimes\cdots\otimes A_s$。$A_i(i=1,2,\cdots,s)$称做$G$的直积因子。

多个子群的直积也和两个子群的直积一样具有下述性质：直积因子的次序可以更换；G的阶等于各直积因子的阶的乘积；从各直积因子的交换性可以推出G的交换性。同样地，任意元素表法的唯一性也可以从单位元素表法的唯一性推出。

从定义可以看出，如果

$$G=A\otimes B,\quad A=A_1\otimes A_2,\quad B=B_1\otimes B_2.$$

那么

$$G=A_1\otimes A_2\otimes B_1\otimes B_2.$$

反之，如果

$$G=A_1\otimes A_2\otimes B_1\otimes B_2,$$

那么，令

$$A=A_1\otimes A_2,\quad B=B_1\otimes B_2.$$

就有

$$G=A\otimes B.$$

即 $$G=(A_1\otimes A_2)\otimes(B_1\otimes B_2).$$

所以在多个子群的直积中，可以任意添加或减少括号。

最后，和两个子群的直积相仿，多个子群的直积也有与定理1类似的结论：

定理 2 $A_1, A_2, \cdots, A_s (s \geq 2)$ 是 G 的子群。

$$G = A_1 \otimes A_2 \otimes \cdots \otimes A_s$$

的充分必要条件是

(1) $A_1, A_2, \cdots, A_s$ 都是 G 的正规子群；

(2) $G = A_1 A_2 \cdots A_s$；

(3) $A_1 \cdots A_{i-1} A_{i+1} \cdots A_s \cap A_i = \{e\}$，$i = 1, 2, \cdots, s$。

这个定理的证明与定理1的证明差不多，这里就不重复了。

利用子群的直积这个概念可以将群的一些问题化为子群的问题来研究。例如，群的运算可以归结为子群的运算，设

$$G = A_1 \otimes A_2 \otimes \cdots \otimes A_s$$

$$g = g_1 g_2 \cdots g_s, \quad g_i \in A_i \ (i = 1, 2, \cdots, s);$$

$$h = h_1 h_2 \cdots h_s, \quad h_i \in A_i \ (i = 1, 2, \cdots, s).$$

那么

$$gh = (g_1 h_1)(g_2 h_2) \cdots (g_s h_s), \quad g_i h_i \in A_i \ (i = 1, 2, \cdots, s).$$

又如上面已经提到过，G 的交换性可以从 A_i 的交换性得出。更进一步，我们有：如果 $Z, Z_1, Z_2, \cdots, Z_s$ 分别是 $G, G_1, G_2, \cdots, G_s$ 的中心，那么有

$$Z = Z_1 \otimes Z_2 \otimes \cdots \otimes Z_s.$$

证明留作习题。

下一节我们将讨论交换群的直积分解。通过对交换群的讨论，我们对于直积分解的作用将有进一步的体会。

§2 基

这一节我们介绍交换群的基的概念，并利用这个概念来得到有限交换群的直积分解。

设 G 是一个交换群，任取 G 中一组元素 $a_1, a_2, \cdots, a_s$。形如

$$a_1^{k_1} a_2^{k_2} \cdots a_s^{k_s} \quad (k_1, k_2, \cdots, k_s \text{ 是任意整数})$$

的元素全体组成 G 的一个子群，称为 G 的**由 $a_1, a_2, \cdots, a_s$ 生成的子群**，记作 $\langle a_1, a_2, \cdots, a_s \rangle$。如果 $a_1, a_2, \cdots, a_s$ 生成的子群就是 G，就称 $a_1, a_2, \cdots, a_s$ 是 G 的一组**生成元**。有限交换群总有生成元，问题是如何选择生成元，使包含的元素个数最少。

定义 3 设 $a_1, a_2, \cdots, a_s$ 是交换群 G 中的一组元素。如果从

$$a_1^{k_1} a_2^{k_2} \cdots a_s^{k_s} = e$$

可推出

$$a_i^{k_i} = e, \quad i = 1, 2, \cdots, s,$$

就称 $a_1, a_2, \cdots, a_s$ 是**无关的**。G 的一组无关的生成元称做 G 的一组**基**。

例 1 $G = \{e, (\alpha_1, \alpha_2)(\alpha_3, \alpha_4), (\alpha_1, \alpha_3)(\alpha_2, \alpha_4),$
$(\alpha_1, \alpha_4)(\alpha_2, \alpha_3), (\beta_1, \beta_2, \beta_3), (\beta_1, \beta_3, \beta_2),$
$(\alpha_1, \alpha_2)(\alpha_3, \alpha_4)(\beta_1, \beta_2, \beta_3),$
$(\alpha_1, \alpha_3)(\alpha_2, \alpha_4)(\beta_1, \beta_2, \beta_3),$
$(\alpha_1, \alpha_4)(\alpha_2, \alpha_3)(\beta_1, \beta_2, \beta_3),$
$(\alpha_1, \alpha_2)(\alpha_3, \alpha_4)(\beta_1, \beta_3, \beta_2),$
$(\alpha_1, \alpha_3)(\alpha_2, \alpha_4)(\beta_1, \beta_3, \beta_2),$

$$(\alpha_1,\alpha_4)(\alpha_2,\alpha_3)(\beta_1,\beta_3,\beta_2)\}.$$

很容易看出

$$(\alpha_1,\alpha_2)(\alpha_3,\alpha_4),\quad (\alpha_1,\alpha_3)(\alpha_2,\alpha_4),\quad (\beta_1,\beta_2,\beta_3)$$

是G的一组生成元，而且从

$$[(\alpha_1,\alpha_2)(\alpha_3,\alpha_4)]^l[(\alpha_1,\alpha_3)(\alpha_2,\alpha_4)]^m(\beta_1,\beta_2,\beta_3)^k=e$$

可推出

$$l\equiv 0 \pmod 2,\quad m\equiv 0 \pmod 2,\quad k\equiv 0 \pmod 3.$$

即

$$(\alpha_1,\alpha_2)(\alpha_3,\alpha_4)^l=[(\alpha_1,\alpha_3)(\alpha_2,\alpha_4)]^m=(\beta_1,\beta_2,\beta_3)^k=e.$$

所以这三个元素组成G的一组基。

G的基不是唯一的，读者可以自己再找出G的另一组基。

交换群的基有下述一些性质：

1．如果$G=A\otimes B$，$a_1,a_2,\cdots,a_s$是A的一组基，$b_1,b_2,\cdots,b_t$是B的一组基，那么$a_1,\cdots,a_s,b_1,\cdots,b_t$是$G$的一组基。

2．如果$a_1,a_2,\cdots,a_s$是G的一组基，设$a_1,a_2,\cdots,a_l$ $(0<l<s)$生成的子群是A；$a_{l+1},a_{l+2},\cdots,a_s$生成的子群是$B$，那么

$$G=A\otimes B.$$

特别地，有

$$G=\langle a_1\rangle\otimes\langle a_2\rangle\otimes\cdots\otimes\langle a_s\rangle.$$

其中$\langle a_i\rangle$是a_i生成的循环群。

这两条性质可以从基的定义和直积的性质直接推出，从这两条性质可以看到交换群的直积分解与基的选择有密切的关系。下面对交换群证明基的存在。

定理 3　有限交换群一定有基。

证明　设G是一个有限交换群。$a_1,a_2,\cdots,a_r$是G的一组生成元。我们对r作归纳法。

当$r=1$时，G是由a_1生成的循环群，a_1就是G的一组基。

当$r\geqslant 2$时，设定理对于具有一组元素个数少于r的生成元的有限交换群成立。来证定理对于由r个元素生成的群也成立。

在所有使

$$a_1^{k_1}a_2^{k_2}\cdots a_r^{k_r}=e$$

成立的k_i中有一个最小的正整数，设为m，我们再对m作归纳法。

可以调动a_i的次序使m是a_1的指数。于是有整数$m_2,\cdots,m_r$使

$$a_1^{m}a_2^{m_2}\cdots a_r^{m_r}=e. \qquad (1)$$

如果$m=1$，那么

$$a_1=a_2^{-m_2}\cdots a_r^{-m_r}.$$

G可以由$r-1$个元素$a_2,a_3,\cdots,a_r$生成，由归纳法假设G有基。

下面设$m>1$。将m_i表成

$$m_i=t_im+s_i,\quad 0\leqslant s_i<m\ (i=2,\cdots,r).$$

令

$$a_1^*=a_1a_2^{t_2}\cdots a_r^{t_r}. \qquad (2)$$

由（1），（2）两式得

$$(a_1^*)^m a_2^{s_2}\cdots a_r^{s_r}=e.$$

如果$s_i(i=2,\cdots,r)$中有一个不等于0，那么它一定小于m，对这个s_i应用归纳法假设，知G有基。因此可设

$$s_2=s_3=\cdots=s_r=0,$$

此时有 $(a_1^*)^m = e$。

因为 a_1 可以用 $a_1^*, a_2, \cdots, a_r$ 表示：

$$a_1 = a_1^* a_2^{-t_2} \cdots a_r^{-t_r}.$$

所以 $a_1^*, a_2, \cdots, a_t$ 也是 G 的一组生成元，我们来证明

$$G = \langle a_1^* \rangle \otimes \langle a_2, \cdots, a_r \rangle.$$

根据定理 1，为了证明这个分解式，只要证明

$$\langle a_1^* \rangle \cap \langle a_2, \cdots, a_r \rangle = \{e\}.$$

任取 $a \in \langle a_1^* \rangle \cap \langle a_2, \cdots, a_r \rangle$。那么 a 可以表成

$$a = (a_1^*)^l = (a_1 a_2^{t_2} \cdots a_r^{t_2})^l = a_2^{l_2} \cdots a_r^{l_r}.$$

于是 $$a_1^l a_2^{t_2 l - l_2} \cdots a_r^{t_r l - l_r} = e. \qquad (3)$$

对于整数 l, m，可以找到整数 x 使

$$0 \leqslant l - xm < m.$$

由（1），（3）两式得

$$a_1^{l-xm} a_2^{t_2 l - l_2 - xm_2} \cdots a_r^{t_r l - l_r - xm_r} = e.$$

根据 m 的选择，必须有

$$l - xm = 0.$$

因此 $$a = (a_1^*)^l = (a_1^*)^{xm} = e.$$

这样就证明了 $G = \langle a_1^* \rangle \otimes \langle a_2, \cdots, a_r \rangle$。

因为 $\langle a_2, \cdots, a_r \rangle$ 可以由 $r-1$ 个元素生成，根据归纳法假设，$\langle a_2, \cdots, a_r \rangle$ 有一组基，设为 $b_2, \cdots, b_u$。于是 $a_1^*, b_2, \cdots, b_u$ 就是 G 的一组基，定理证毕。▎

根据有限交换群的基的存在性，可以得到下列推论。

推论 任一有限交换群都可以表成循环群的直积。

设 G 是一个有限群，在 G 中取定一组基 $a_1, a_2, \cdots, a_s$。那么

$$G = \langle a_1 \rangle \otimes \langle a_2 \rangle \otimes \cdots \otimes \langle a_s \rangle.$$

设 a_i 的阶为 $n_i (i = 1, 2, \cdots, s)$。那么 G 中任一元素 g 都可唯一地表成

$$g = a_1^{k_1} a_2^{k_2} \cdots a_s^{k_s}, \quad 0 \leqslant k_i < n_i \quad (i = 1, 2, \cdots, s).$$

如果 h 也是 G 中一个元素，设

$$h = a_1^{l_1} a_2^{l_2} \cdots a_s^{l_s}, \qquad 0 \leqslant l_i < n_i \ (i = 1, 2, \cdots, n).$$

那么

$$gh = a_1^{m_1} a_2^{m_2} \cdots a_s^{m_s}.$$

式中的 m_i 满足

$$m_i \equiv h_i + l_i \pmod{n_i}, \quad 0 \leqslant m_i < n_i, \quad i = 1, 2, \cdots, s.$$

在下一节中我们将进一步讨论有限交换群的直积分解。

§3 有限交换群的构造

我们以前讨论过循环群，循环群可以由一个元素生成，它的构造是很简单的。上一节我们通过基的存在性，证明了有限交换群可以表成循环子群的直积，这一节我们进一步来证明有限交换群可以分解成阶为素数的方幂的循环子群的直积，而且表法是唯一的。这样就完全解决了有限交换群的构造问题。

我们先来证明一个更为一般的结论。设 G 是一个有限交换群，用 $G(p)$ 表示 G 中阶为素数 p 的方幂的元素全体，那么 $G(p)$ 显然是非空集合，而且对 G 的运算是封闭的，所以 $G(p)$ 是 G 的一个子群。

定理 4 设 G 是一个 n 阶交换群，$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$，其中 $p_1, \cdots, p_s$ 是两两不同的素数，$\alpha_i > 0$ $(i = 1, 2, \cdots, s)$，那么

$$G = G(p_1) \otimes G(p_2) \otimes \cdots \otimes G(p_s).$$

为了证明定理 4，需要用到一个结果，这个结果在任何群中都是成立的，我们把它写成一个引理。

引理 设 a 是群 G 中一个元素，a 的阶等于 $m=m_1m_2$。其中 m_1 与 m_2 是两个互素的正整数，那么 a 可以唯一地表成 $a=a_1a_2$，式中 a_i 的阶是 $m_i(i=1,2)$；$a_1a_2=a_2a_1$；而且 $a_i(i=1,2)$ 都是 a 的方幂。

证明 因为 m_1 与 m_2 互素，故有整数 u_1,u_2 使得

$$u_1m_1+u_2m_2=1。$$

于是

$$a=a^{u_1m_1+u_2m_2}=a^{u_1m_1}\cdot a^{u_2m_2}=a^{u_2m_2}\cdot a^{u_1m_1}。$$

令 $$a_1=a^{u_2m_2},\quad a_2=a^{u_1m_1}。$$

则 a_1,a_2 都是 a 的方幂，而且

$$a=a_1a_2=a_2a_1。$$

下面来看 a_1,a_2 的阶。因为

$$a_1^{m_1}=a^{u_2m_2m_1}=e,\quad a_2^{m_2}=a^{u_1m_1m_2}=e。$$

所以 a_1 的阶是 m_1 的一个因子 d_1，a_2 的阶是 m_2 的一个因子 d_2。由于 a_1 与 a_2 可交换，并且 d_1 与 d_2 互素，故 a_1a_2 的阶等于 d_1d_2。但是已知 a 的阶是 m_1m_2，所以必须有

$$d_1=m_1,\quad d_2=m_2。$$

最后来证表法的唯一性。设

$$a=a_1a_2=a_1'a_2',$$

其中 a_1,a_2,a_1',a_2' 都满足条件。那么

$$a_1^{-1}a_1'=a_2'a_2^{-1}。$$

因为 a_1,a_1' 都是 a 的方幂，所以它们可以交换，于是 $a_1^{-1}a_1'$ 的阶是 m_1 的因子，同样可知 $a_2'a_2^{-1}$ 的阶是 m_2 的因子。由假设知 m_1 与 m_2 互素，故必有

$$a_1^{-1}a_1'=a_2'a_2^{-1}=e。$$

从而 $$a_1=a_1',\qquad a_2=a_2'。$$

唯一性得证。❙

反复应用引理，可以得到 m 分解成几个互素的因子的一般情形：

设 a 是群 G 中一个元素，a 的阶为 $m=m_1m_2\cdots m_r(r\geqslant 2)$，其中 $m_1,m_2,\cdots,m_r$ 是两两互素的正整数，那么 a 可以唯一地表成

$$a=a_1a_2\cdots a_r。$$

其中 a_i 的阶为 m_i，$a_ia_j=a_ja_i$，而且 a_i 都是 a 的方幂$(i,j=1,2,\cdots,r)$。

定理 4 可以从这个结论直接得出。

因为 $G(p_i)$ 中元素的阶都是 p_i 的方幂，故由定理 3 及其推论可知 $G(p_i)$ 的阶也是 p_i 的方幂。又因

$$|G|=\prod_{1<i<s}|G(p_i)|,$$

所以可得

$$|G(p_i)|=p_i^{e_i},\quad i=1,2,\cdots,s。$$

定义4 如果群 G 中一个元素 g 的阶为素数 p 的一个方幂，则称 g 为一个 **p-元素**。如果群 G 的阶是素数 p 的一个方幂，则称 G 为一个 **p-群**。

因为群中元素的阶为这个群的阶的因子，故 p-群中的元素都是 p-元素。以后我们将看到，如果有限群 G 中每个元素都是 p-元素，那么 G 一定是一个 p-群。因此 p-群也可以定义为其元素皆为 p-元素的群。

定义5 设群 G 的阶为 $n=p^an_1$，p 是一个素数，n_1 与 p 互素。那么 G 的 p^a 阶子群称为 G 的一个 **Sylow p-子群**。

定理 4 说明：当 G 是 n 阶有限交换群的时候，对于 n 的每个素因子 p，G 的 Sylow p-子群都是存在且唯一的。而且 G 可以表成它的 Sylow p-子群的直积。

从定理 4 以及上节的结果，还可以知道任一有限交换群都可以表成循环p-子群的直积。下面来证明表法是唯一的。

首先对表法的唯一性作一点说明，先来看两个例子。

例1 G是上节例 1 中的群，已知G有一组基是

$$(\alpha_1,\alpha_2)(\alpha_3,\alpha_4),(\alpha_1,\alpha_3)(\alpha_2,\alpha_4),\ (\beta_1,\beta_2,\beta_3),$$

所以G可以分解成循环 2-子群

$$\langle(\alpha_1,\alpha_2)(\alpha_3,\alpha_4)\rangle,\langle(\alpha_1,\alpha_3)(\alpha_2,\alpha_4)\rangle$$

及循环 3-子群$\langle(\beta_1,\beta_2,\beta_2)\rangle$的直积。

$$G=\langle(\alpha_1,\alpha_2)(\alpha_3,\alpha_4)\rangle\otimes\langle(\alpha_1,\alpha_3)(\alpha_2,\alpha_4)\rangle\otimes\langle(\beta_1,\beta_2,\beta_2)\rangle.$$

很容易看出G还有另一种分解：

$$G=\langle(\alpha_1,\alpha_2)(\alpha_3,\alpha_4)\rangle\otimes\langle(\alpha_1,\alpha_4)(\alpha_2,\alpha_3)\rangle\otimes\langle(\beta_1,\beta_2,\beta_3)\rangle.$$

例2 设G是由 6 阶元素 a 及 4 阶元素 b 生成的 24 阶交换群，那么

$$G=\langle a\rangle\otimes\langle b\rangle.$$

但是$\langle a\rangle$的阶不是素数的方幂，我们再把G进一步分解：

$$G=\langle a^3\rangle\otimes\langle a^2\rangle\otimes\langle b\rangle.$$

G就表成了循环p-子群的直积。G还可以分解成：

$$G=\langle a^3b^2\rangle\otimes\langle a^2\rangle\otimes\langle a^3b\rangle.$$

这也是循环p-子群的直积。

这两个例子说明同一个交换群可以用几种方法分解成循环p-子群的直积。但是我们可以看出在同一个群的不同分解式中，直积因子的个数和阶都是一样的。所谓表法的唯一性就是指的这个事实。

因为在直积分解中可以交换直积因子的次序并且可以随意添加或去掉括号，所以我们只要对交换p-群来证明分解的唯一性。

定理5 设有限交换p-群G用两种方法表成循环 p-群的直积：

$$G=A_1\otimes A_2\otimes\cdots\otimes A_r=B_1\otimes B_2\otimes\cdots\otimes B_s.$$

那么必有$r=s$，而且可以适当地排列 B_i 的次序使得 B_i 与A_i $(i=1,2,\cdots,r)$有相同的阶。

证明 我们对G的阶作归纳法，当$|G|=p$时定理显然成立。

用G_p表示G中满足$a^p=e$的元素全体组成的子群。用G^p表示G中形如$b^p(b\in G)$的全体元素组成的子群。

用 a_i 表示$A_i(i=1,2,\cdots,r)$的一个生成元。那么 $a_1,a_2,\cdots,a_r$是G的一组基，设a_i的阶是p^{e_i} $(i=1,2,\cdots,r)$，并设(必要时可调动A_i的次序)

$$e_1\geqslant e_2\geqslant\cdots\geqslant e_r\geqslant 1.$$

于是$a_1^{p^{e_1-1}},a_2^{p^{e_2-1}},\cdots,a_r^{p^{e_r-1}}$是$G_p$的一组基，$G_p$ 的阶为p^r。如果$e_1=\cdots e_r=1$，那么$G^p=\{e\}$，否则如果

$$e_1\geqslant e_2\geqslant\cdots\geqslant e_m>e_{m+1}=\cdots=e_r=1$$
$$(1\leqslant m\leqslant r),$$

那么$a_1^p,a_2^p,\cdots,a_m^p$就是G^p的一组基。

B_i的生成元b_i $(i=1,2,\cdots,s)$给出G的另一组基$b_1,b_2,\cdots,b_s$。设b_i的阶是p^{f_i}并调动B_i 的 次序使 $f_1\geqslant f_2\geqslant\cdots\geqslant f_r=1$。如上可知$G_p$的阶等于$p^s$。所以必有$r=s$。如果$G^p=\{e\}$，那么必有 $f_1=f_2=\cdots=f_s=1$。定理得证。如果$G^p\neq\{e\}$，那么设

$$f_1\geqslant f_2\geqslant\cdots\geqslant f_{m'}>f_{m'+1}=\cdots=f_r=1$$
$$(1\leqslant m'\leqslant r).$$

则$b_1^p,b_2^p,\cdots,b_{m'}^p$是$G^p$的另一组基，$G^p$有两种方法表成循环子群的直积：

$$G^p = \langle a_1^p\rangle \otimes \langle a_2^p\rangle \otimes \cdots \otimes \langle a_m^p\rangle$$
$$= \langle b_1^p\rangle \otimes \langle b_2^p\rangle \otimes \cdots \otimes \langle b_{m'}^p\rangle.$$

因为G^p的阶小于G的阶，对G^p应用归纳法假设可得$m = m'$而且$\langle a_i^p\rangle$与$\langle b_i^p\rangle$ $(i = 1, 2, \cdots, m)$有相同的阶，因此 a_i 与 $b_i (i = 1, 2, \cdots, s)$ 也有相同的阶，即 A_i与B_i $(i = 1, 2, \cdots, s)$ 有相同的阶。 ▎

由此可得出关于有限交换群的基本定理：

定理6 有限交换群可以唯一地表成循环 p- 群的直积。

定理 6 也说明了有限交换群的由阶为素数幂的元素组成的基中元素的个数及其阶的唯一性，由此引入下述概念。

定义6 如果有限交换群G可以表成循环p-群 $G_1, G_2, \cdots, G_s$的直积，G_i的阶为n_i $(i = 1, 2, \cdots, s)$，则$n_1, n_2, \cdots, n_s$称为 G **的不变量**。如果 G 的不变量都是素数，那么 G 称为**初等交换群**。

推论 两个有限交换群同构的充分必要条件是它们的不变量相同。

例3 例 1 中 G 的不变量是$2, 2, 3$，所以 G 是一个初等交换群。

例4 由置换$(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$，$(\beta_1, \beta_2, \beta_3)$生成的群是12阶交换群，它的不变量是$2^2$，3。这个群与上题中的$G$不同构。

例5 p^4阶交换群的不变量有下述五种可能：

$$p, p, p, p;\quad p^2, p, p;\quad p^2, p^2;\quad p^3, p;\quad p^4.$$

所以p^4阶交换群在同构的意义下共有 5 个。

下面来说明交换群的不变量与其子群的不变量之间的关系。

定理7 设G是一个交换p-群，它的不变量是$p^{e_1}, p^{e_2}, \cdots, p^{e_s} (e_1 \geqslant e_2 \geqslant \cdots \geqslant e_s \geqslant 1)$，则$G$有以 $p^{f_1}, p^{f_2}, \cdots, p^{f_t} (f_1 \geqslant f_2 \geqslant \cdots \geqslant f_t \geqslant 1)$为不变量的子群的必要充分条件是 $t \leqslant s$，并且$f_i \leqslant e_i$ $(i = 1, 2, \cdots, t)$。

证明 首先来证明G的子群H 的不变量 $p^{f_1}, p^{f_2}, \cdots, p^{f_t}$ $(f_1 \geqslant f_2 \geqslant \cdots \geqslant f_t \geqslant 1)$满足定理中的条件。

对G的阶作归纳法。当$|G| = p$时，结论显然是成立的。

设G的阶大于p，如果G 是初等交换群，那么H也是初等交换群，此时

$$e_1 = e_2 = \cdots = e_s = 1;\quad f_1 = f_2 = \cdots = f_t = 1.$$

比较G与H的阶即得$t \leqslant s$。所以结论是成立的。如果G 不是初等交换群，则G_p是p^s阶初等交换群，H_p是p^t阶初等交换群。所以有$t \leqslant s$。再设

$$e_1 \geqslant e_2 \geqslant \cdots \geqslant e_m > e_{m+1} = \cdots = e_s = 1,$$
$$f_1 \geqslant f_2 \geqslant \cdots \geqslant f_l > f_{l+1} = \cdots = f_t = 1.$$

于是G^p的不变量是 $p^{e_1-1}, p^{e_2-1}, \cdots, p^{e_m-1}$ $(e_1 - 1 \geqslant e_2 - 1 \geqslant \cdots \geqslant e_m - 1 \geqslant 1)$，$H^p$的不变量是

$$p^{f_1-1}, p^{f_2-1}, \cdots, p^{f_l-1}\quad (f_1 - 1 \geqslant f_2 - 1 \geqslant \cdots \geqslant f_l - 1 \geqslant 1).$$

因为H^p是G^p的子群而且G^p的阶小于G的阶。故由归纳法假设，有

$$l \leqslant m;\quad f_i - 1 \leqslant e_i - 1,\quad i = 1, 2, \cdots, l.$$

又因 $$f_{l+1} = \cdots = f_t = 1,$$

所以 $$f_i \leqslant e_i,\quad i = l+1, \cdots, t.$$

因此有 $$f_i \leqslant e_i,\quad i = 1, 2, \cdots, t.$$

再证如果$f_1, f_2, \cdots, f_t$满足定理中的不等式，一定存在以p^{f_1}，$p^{f_2}, \cdots, p^{f_t}$为不变量的子群。设$a_1, a_2, \cdots, a_s$是 G 的一组基，它们的阶依次为$p^{e_1}, p^{e_2}, \cdots, p^{e_s}$。

令 $$b_i = a_i^{p^{e_i - f_i}},\quad i = 1, 2, \cdots, t.$$

则b_i的阶为$p^{f_i} (i = 1, 2, \cdots, t)$。

$$H=\langle b_1\rangle\otimes\langle b_2\rangle\otimes\cdots\otimes\langle b_t\rangle$$

就是G的一个以$p^{f_1},p^{f_2},\cdots,p^{f_t}$为不变量的子群。▎

定理 7 可以推广到更一般的情形：设交换群G的不变量是

$$p_1^{e_{11}},\cdots,p_1^{e_{1s_1}},p_2^{e_{21}},\cdots,p_2^{e_{2s_2}},\cdots,p_u^{e_{u1}},\cdots,p_u^{e_{us_u}},$$

其中　　$s_i>0$；$e_{i1}\geqslant e_{i2}\geqslant\cdots\geqslant e_{is_i}$　$(i=1,2,\cdots,u)$。

则G有以

$$p_1^{f_{11}},\cdots,p_1^{f_{1t_1}},p_2^{f_{21}},\cdots,p_2^{f_{2t_2}},\cdots,p_u^{f_{u1}},\cdots,p_u^{f_{ut_u}},$$

其中　　$t_i\geqslant 0$；$f_{i_1}\geqslant f_{i_2}\geqslant\cdots\geqslant f_{it_i}$　$(i=1,2,\cdots,u)$

为不变量的子群的充分必要条件是

$$t_i\leqslant s_i,\ 并且 f_{ij}\leqslant e_{ij}\ (i=1,2,\cdots,u;j=1,2,\cdots,t_i)。$$

由此可以看出：如果G是一个n阶交换群，那么对于n的任一个正因子m，G都有m阶子群，这个结论当G非交换时是不成立的。

最后，我们来证明循环群的一个重要性质，我们知道，如果G是一个n阶循环群，那么对于n的任一个正因数m，G都恰有一个m阶子群。特别的，对n的素因数p，G恰有一个p阶子群。这个性质也是一个交换群为循环群的充分条件。即有：

定理8　设G是一个交换p-群，如果G只有一个p阶子群，那么G是一个循环群。

证明　设G的不变量为$p^{e_1},p^{e_2},\cdots,p^{e_s}$。如果$s>1$，则$G$有一组基$a_1,a_2,\cdots,a_s$。其中$a_i$的阶为$p^{e_i}$　$(i=1,2,\cdots,s)$。

令　　　　$H_1=\langle a_1^{p^{e_1-1}}\rangle$，$H_2=\langle a_2^{p^{e_2-1}}\rangle$。

则H_1与H_2是G的两个不同的p阶子群，与假设矛盾。因此$s=1$，G是循环群。▎

这个结论可以推广到一般交换群的情形(参考习题13)。

这个结论对非交换群是不成立的。例如，四元数群只有一个 2 阶子群，但是它不是交换群，当然更不可能为循环群。

习　　题

1.　设$G=G_1\otimes G_2$，$A_1\triangleleft G_1$，$A_2\triangleleft G_2$。求证：

$$A_1\otimes A_2\triangleleft G。$$

2.　设$G=G_1\otimes G_2$，$H=H_1\otimes H_2$　并且

$$G_1\cong G_2,\ H_1\cong H_2。$$

求证：$G\cong H$。

3.　$G=A\otimes B$。已知$|A|$与$|B|$互素，求证A与B都是G的特征子群。

4.　证明：$(G\otimes H)_p=G_p\otimes H_p$；

$$(G\otimes H)^p=G^p\otimes H^p。$$

5.　证明：$(A\otimes B)'=A'\otimes B'$。

6.　G是一个交换p群。i是一个正整数。令

$$p_i(G)=\{a\in G|a^{p^i}=1\},$$

$$p^i(G)=\{a^{p^i}|a\in G\}。$$

证明：

(1)　$p_i(G)$及$p^i(G)$都是G的子群。

(2)　$G/p^i(G)\cong p^i(G)$。

(3)　$G/p^i(G)\cong p_i(G)$。

7.　$p_i(G)$的定义如上题。再设

$$|p^i(G):p^{i-1}(G)|=p^{s_i}。$$

求证$n_i \geqslant n_{i+1}$ ($i=1,2,\cdots$)。

8． 设G是由$(a_1,a_2,a_3,a_4,a_5,a_6)$，$(a_7,a_8)$生成的 8 次置换群。

(1) 求G的两组基。

(2) 将G表成循环p-群的直积。

9． 已知交换p群G的不变量为p^3,p^2。问G有多少个p阶子群，多少个p^2阶子群，多少个p^2阶循环子群？

10． 证明：交换p群可以由它的全部最高阶元素生成。

11． G是一个p群，它的不变量是p,p^{n-1}，m是一个小于n的正整数。证明：

(1) G共有$p+1$个p^m阶子群。

(2) 当$m=1$时，G共有$p+1$个p^m阶循环子群；当$m>1$时，G共有p个p^m阶循环群。

12． G是一个有限交换群。证明G有一组基$a_1,a_2,\cdots,a_s$，它们的阶$n_1,n_2,\cdots,n_s$满足

$$n_i \mid n_{i+1}, \quad i=1,2,\cdots,s。$$

13． G是一个交换群。如果对$|G|$的每个素因数p，G都恰有一个p阶子群，那么G是一个循环群。

14． G是一个p群，如果G的指数为p的子群只有一个，那么G是一个循环群。

15． 把上题中的结论推广到一般有限交换群的情形并加以证明。

16． 证明：p^n阶交换群的自同构群的阶可被p^{n-1}整除。

17． G是一个p^n阶循环群，求$A(G)$的阶。

18． 定出180阶交换群的所有可能的型。

19 证明：如果交换群G有m，n阶元素，则G有$[m,n]$阶元素($[m,n]$表示m与n的最小公倍数)。

20． 证明：有限交换群G是循环群的充分必要条件是G的阶等于G中一切元素的阶的最小公倍数。

第五章　Sylow 定理

我们知道，n阶群的子群的阶一定是n的一个因数，而且，对于n阶交换群来说，如果m是n的一个正因数，那么G一定有m阶子群。但是这个结论对于非交换群是不成立的。例如4元交错群A_4的阶等于12，我们已知A_4有阶为1，2，3，4及12的子群，但是A_4没有6阶子群。

然而，如果n的因数m是一个素数的方幂，那么n阶群G一定有m阶子群。特别地，G一定有Sylow p-子群。

这一章的内容主要是证明G的p-子群的存在；讨论Sylow p-子群的个数及其共轭性，并且讨论G可以表成Sylow p-子群的直积的条件，最后讨论了有限p-群的构造并介绍了一些特殊p-群。

§1　Sylow定理

定理1（第一Sylow定理）　设群G的阶为$n=p^a m$，其中p是一个素数，$a\geqslant 1$，$(p,m)=1$。则G有p^i $(i=1,2,\cdots,a)$阶子群。特别地，G有Sylow p-子群。

证明　对G的阶作归纳法。如果$n=p$，结论显然成立。设结论对于阶小于n的群成立。

用Z表示G的中心，并设Z的阶为z。如果$p|z$，那么Z中一定有一个p阶元素a。于是$\langle a\rangle$是G的一个p阶正规子群。G关于$\langle a\rangle$的商群$G/\langle a\rangle$的阶为$p^{a-1}m$，小于n。由归纳法假设，$G/\langle a\rangle$有p^i $(i=1,2,\cdots,a-1)$阶子群$P_i/\langle a\rangle$。因此，P_i是G的p^{i+1} $(i=1,2,\cdots,a-1)$阶子群。

如果$p\nmid z$。考虑G的共轭元素类。设G的非中心元素分成s个类，它们的元素数分别是$h_1,h_2,\cdots,h_s$，那么

$$n=z+\sum_{i=1}^{s}h_i.$$

因为$p|n$，$p\nmid z$，所以一定有一个$h_t(1\leqslant t\leqslant s)$不能为$p$整除。设$b$是这个共轭类中的一个元素，用$N$表示$b$在$G$内的中心化子。那么$N$的指数为

$$|G:N|=h_k>1.$$

并且$p^a\,||N|$。因为$|N|<n$，故由归纳法假设N有p^i $(i=1,2,\cdots,a)$阶子群P_i。P_i也是G的p^i $(i=1,2,\cdots,a)$阶子群。▌

由定理1可以得到下述重要结论。

推论　如果素数p能整除有限群G的阶，那么G中一定有p阶元素。

定理2（第二Sylow定理）　G的Sylow p-子群都是共轭的。G的Sylow p-子群的个数可以表成$1+kp$，而且是G的阶n的一个因数。

证明　设$P,P_1,P_2,\cdots,P_r$是G的全部Sylow p-子群。因为Sylow p-子群的共轭子群一定也是Sylow p-子群。所以对于G的任一个元素a，可以定义一个$r+1$元置换σ_a：

$$\sigma_a=\begin{pmatrix}P & P_1 & \cdots & P_r\\ a^{-1}Pa & a^{-1}P_1a & \cdots & a^{-1}P_ra\end{pmatrix}$$

令

$$S_P=\{\sigma_a|a\in P\}.$$

S_P是P的一个同态象，因此也是一个p-群。

如果$P_t(1\leqslant t\leqslant r)$在$S_P$下不变，那么对任一$a\in P$，都有$aP_t=P_ta$，因此$PP_t$是$G$的一个$p$-子群。由于$P,P_t$都是Sylow p-子群，必有$PP_t=P=P_t$，这是不可能的。因此P是S_P的

唯一的不动点。其它r个$P_i(i=1,2,\cdots,r)$分别属于S_P的一些传递集。每个传递集中子群的个数都是$|S_P|$的因数，而且不等于1。因为$|S_P|$是一个p幂，所以r是p的一个倍数。G的Sylow p-子群的总数可以表成$1+kp$。

设与P共轭的子群共有s个，可以同前面一样地证明$s\equiv 1 \pmod p$。如果G还有另一个共轭Sylow p-子群类，其中包含s_1个子群，那么这s_1个子群可以分成S_P的一些传递集，因此$p|s_1$。但是和s一样，$s_1\equiv 1 \pmod p$。这是一个矛盾。所以G只能有一个共轭Sylow p-子群类，即G的所有的Sylow p-子群都是共轭的。

因为所有Sylow p-子群组成一个共轭类，所以它们的总数$1+kp$一定是n的一个因数。 ▎

推论 设P是G的一个Sylow p-子群。则

(1) P是G的正规子群的充分必要条件是P是G的唯一的Sylow p-子群。

(2) P是$N_G(P)$的唯一的Sylow p-子群。

定理3(第三 Sylow 定理) G的任一个p-子群A都包含在一个Sylow p-子群中。

证明 仍用σ_a表示定理2的证明中所定义的$r+1$元置换。令

$$S_A=\{\sigma_a \mid a\in A\}.$$

那么G的Sylow p-子群$P=P_0,P_1,\cdots,P_r$分成S_A的一些传递集。这些传递集中包含的Sylow p-子群的个数或者是1，或者是p的一个不等于1的方幂。但是因为$r\equiv 1 \pmod p$，所以至少有一个传递集只包含一个Sylow p-子群，设为$P_l(0\leqslant l\leqslant r)$。于是对$A$中任一个元素$a$，都有

$$a^{-1}P_l a=P_l.$$

于是AP_l是一个p-群，比较P_l及AP_l的阶，即得

$$AP_l=P_l.$$

因此
$$A\leqslant P_l. \quad ▎$$

在进一步讨论Sylow子群的其它性质以前，我们先来举例说明Sylow定理的一些应用。

例1 如果G的阶为$2n$，n是一个奇数，那么G一定有指数为2的正规子群。

证明 用R_G表示G的右正则表示。R_G是G的一个同构象。根据定理1的推论，G中包含一个2阶元素a。a在右正则表示下的象σ_a是一个2阶正则置换，因此是n个不相交的对换的乘积。所以σ_a是一个奇置换。于是R_G中全部偶置换组成R_G的一个指数为2的正规子群R_G^+。因为G与R_G是同构的，所以G也有指数为2的正规子群。 ▎

这个例子说明阶为$2n$（n为奇数）的群不可能是单群。

例2 证明455阶群一定是循环群。

证明 设G是一个455阶群。因为$455=5\times7\times13$。所以由定理1，G有阶为13,7,5的元素。又由定理2，知G的Sylow 13-子群及Sylow 7-子群都只有一个，设为P_{13}及P_7。那么$P_{13}P_7$是G的一个91阶正规子群。考虑G的Sylow 5-子群，由定理2，Sylow 5-子群的个数为1或91。如果G有91个Sylow 5-子群，那么G共有$91\times4=364$个5阶元素。而$P_{13}P_7$中包含91个阶与5互素的元素。这两种元素共有455个，就是G的全部元素。任取一个Sylow 5-子群P_5。则$P=P_7P_5$是G的一个35阶子群。因为

$$P_5\lhd P,\quad P_7\lhd P,\quad P_5\cap P_7=\{e\}.$$

所以

$$P=P_5\otimes P_7.$$

因此P是一个35阶循环群。G包含一个35阶元素。这个元素不在前面所列的455个元素中，这是不可能的。所以G只有一个 Sylow 5-子群P_5。于是

$$G=P_{13}\otimes P_7\otimes P_5.$$

G是一个455阶循环群。❙

例3 60阶单群都与A_5同构。因此在同构的意义下，60阶单群只有一个。

证明 设G是一个60阶单群。由于G是单群，故G的非单位同态象都一定是同构象。因此G对任一真子群的陪集置换表示也一定与G同构。所以我们只要证明G有指数为5的子群。

因为$60>4!$，所以G不可能与S_4的子群同构，所以G没有指数小于5的子群。

考虑G的Sylow子群。因为对同一个素数p，G的Sylow p-子群组成一个共轭子群类，类中子群的总数等于此共轭类中任一子群的正规化子的指数。所以对于$|G|$的任一素因数p，G的 Sylow p-子群的个数都不能少于5个。

因为$60=2^2\times3\times5$，故由上述分析知G的 Sylow 5-子群共有6个。G共有24个5阶元素。

G的 Sylow 2-子群只能是5个或15个(已知不可能是3个)。如果G有5个 Sylow 2-子群，那么G的 Sylow 2-子群的正规化子就是G的指数为5的子群。如果G有15个 Sylow 2-子群。假如G的任两个 Sylow 2-子群之交都是单位子群，那么G将有45个2-元素。但是G已有24个5-元素，所以这是不可能的。因此G一定有两个 Sylow 2-子群P_1,P_2，它们的交是一个2阶子群A。因为4阶群都是交换群，所以

$$P_1,P_2\leqslant Z_G(A)<G.$$

因此$Z_G(A)$的阶是4的倍数且大于4。但是$Z_G(A)$的指数不能为3，故$Z_G(A)$的指数为5。

以上证明了G有指数为5的子群，设为H。G对H的陪集置换表示$S_{G/H}\leqslant S_5$。因为S_5只有一个60阶子群，即A_5，所以$G\cong S_{G/H}\cong S_5$。❙

定理4 如果$G\geqslant H\geqslant N_G(P)\geqslant P$，其中$P$是$G$的一个 Sylow 子群。那么$H$在$G$中的正规化子就等于$H$。即

$$H=N_G(H).$$

证明 设G中元素a使$a^{-1}Ha=H$。来证$a\in H$。

从$a^{-1}Ha=H$可推出$a^{-1}Pa\leqslant H$。因为$a^{-1}Pa$也是H的一个 Sylow 子群，与P共轭。因此存在$b\in H$使$b^{-1}(a^{-1}Ha)b=P$。从而$ab\in N_G(P)\leqslant H$。所以$a\in H$。❙

当$H=N_G(P)$时，可知P的正规化子等于它自己的正规化子。

定理5 如果有限群G的p-子群A不是G的 Sylow p-子群。那么A的正规化子不等于A自己。

证明 如果$p\nmid|G:N_G(A)|$，那么由$p\,|\,|G:A|$，即得

$$N_G(A)\neq A.$$

如果$p\,|\,|G:N_G(A)|$，设$|G:N_G(A)|=pl$，并设$A=A_1,A_2,\cdots,A_{pl}$是与A共轭的全部子群。对$a\in A$，作置换

$$\tau_a=\begin{pmatrix}A_1 & A_2 & \cdots & A_{pl}\\ a^{-1}A_1a & a^{-1}A_2a & \cdots & a^{-1}A_{pl}a\end{pmatrix}.$$

令

$$S_A=\{\tau_a|a\in A\}.$$

S_A是$\{A_1,A_2,\cdots,A_{pl}\}$上的一个置换群，$A$是$S_A$的一个不动点。$A$的$pl$个共轭子群$A_1,A_2,\cdots,A_{pl}$分成$S_A$的一些传递集，每个传递集中子群的个数等于1或$p$的方幂($>1$)。因

此至少有 p 个 A_i 在 S_A 下保持不变，设 A_2 是其中的一个。那么对任一 $a\in A$，都有 $a^{-1}A_2a=A_2$。于是 $A_1\leqslant N_G(A_2)$。由此得 $N_G(A_2)>A_2$。由于 A_1 与 A_2 共轭，故有 $N_G(A_1)>A_1$。❙

从定理5的证明可看出，$p\mid |N_G(A_1):A_1|$。因此有下述一些推论。

推论1 如果群 G 的阶等于 p^am，其中 $a\geqslant 1,(p,m)=1$。则 G 的每个 $p^i(1\leqslant i<a)$ 阶子群都是某个 p^{i+1} 阶子群的正规子群。

推论2 设 P 是一个 p^a 阶 p-群。则 P 的极大子群一定都是 p^{a-1} 阶群，并且都是正规子群。

推论3 p 群的眞子群的正规化子不能等于它自己。

下面来讨论群 G 表成其 Sylow 子群的直积的条件。如果

$$G=P_1\otimes P_2\otimes\cdots\otimes P_s$$

是其 Sylow 子群的直积。那么有 $P_i\trianglelefteq G(i=1,2,\cdots,s)$。如果 G 的每个 Sylow 子群都是正规子群。设 P_i 是 G 的 Sylow p_i-子群 $(i=1,2,\cdots,s)$。则因当 $i\neq j$ 时，P_i 的阶与 P_j 的阶互素，故 P_i 中元素与 P_j 元素可交换。又由定理3知 P_i 包含了 G 的全部 p_i-元素 $(i=1,2,\cdots,s)$。因此 $G=P_1\otimes P_2\otimes\cdots\otimes P_s$。这样就得到

定理6 有限群 G 是其 Sylow 子群的直积的充分必要条件是 G 的 Sylow 子群都是正规子群。

我们还可证明

定理7 有限群 G 是其 Sylow 子群的直积的充分必要条件是 G 沒有眞子群等于它自己的正规化子。

证明 设 G 沒有眞子群等于它自己的正规化子。然而根据定理4，G 的 Sylow 子群 P 的正规化子 $N_G(P)$ 等于它自己的正规化子。因此必须有 $N_G(P)=G$，故 $P\trianglelefteq G$。所以由定理6，G 是 Sylow 子群的直积。

现在设 $G=P_1\otimes P_2\otimes\cdots\otimes P_s$，其中 $P_i(i=1,2,\cdots,s)$ 是 G 的 Sylow p_i-子群。则 P_i 是 G 的唯一的 p_i-子群。G 的 p_i-元素都在 P_i 中，$i=1,2,\cdots,s$。设 H 是 G 的一个眞子群。任取 $g\in G$。由第四章§3的引理知 g 可表成

$$g=g_1g_2\cdots g_s,\quad g_i\in P_i\quad(i=1,2,\cdots,s).$$

而且 g_i 都是 g 的方幂，所以 $g_i\in H$。令

$$H_i=H\cap P_i,\qquad i=1,2,\cdots,s.$$

则有

$$H=H_1\otimes H_2\otimes\cdots\otimes H_s.$$

因为 H 是 G 的眞子群，所以一定有一个 $H_r(1\leqslant r\leqslant s)$ 是 P_r 的眞子群，用 N 表示 H_r 在 P_r 中的正规化子，那么 $N>H_r$，并且

$$H\triangleleft H_1\otimes\cdots\otimes H_{r-1}\otimes N\otimes H_{r+1}\otimes\cdots\otimes H_s.$$

这说明 H 的正规化子不能等于 H，定理证毕。❙

最后来证明关于 Sylow 子群的一个定理，这个定理说明 Sylow 子群在有限群研究中的重要性。

定理8 设 N 是 G 的一个正规子群。P 是 N 的一个 Sylow p-子群，则 $G=N_G(P)N$。

证明 任取 G 中一个元素 a。因为 N 是 G 的正规子群，所以 $a^{-1}Pa\leqslant N$，$a^{-1}Pa$ 也是 N 的一个 Sylow p-子群。故由第二 Sylow 定理，存在 N 中一个元素 b 使得 $b^{-1}(a^{-1}Pa)b=P$。于是 $ab\in N_G(P)$，$a\in N_G(P)N$。因此 $G=N_G(P)N$。❙

§2 有限 p-群

上一节我们证明了有限群的 Sylow 子群的存在。并且证

明了对同一个素数 p，G 的 Sylow p- 子群都是共轭的，因此都是同构的。如果 G 的阶 $n=p_1^{l_1}p_2^{l_2}\cdots p_s^{l_s}$，其中 $p_1,p_2,\cdots,p_s$ 是不同素数；$l_1,l_2,\cdots,l_s$ 是正整数。对每个 $i(1\leqslant i\leqslant s)$ 取定一个 Sylow p_i-子群 P_i。这些 $P_i(i=1,2,\cdots,s)$ 就生成群 G。因此讨论有限 p-群的构造对研究有限群的构造很有用处。在上一节中我们已经涉及有限 p-群的一些结论。这一节再介绍关于有限 p-群的一些基本结论。

定理9 有限 p-群 $G(\neq\{e\})$ 的中心大于 $\{e\}$。

证明 设 $|G|=p^m$。将 G 分解成共轭元素类之并：

$$G=C_1\cup C_2\cup\cdots\cup C_t,\qquad C_i\cap C_j=\varnothing\ (i\neq j).$$

其中 $C_1=\{e\}$。设 C_i 中包含 h_i 个元素 $(i=1,2,\cdots,t)$。那么 h_i 是 p^m 的一个因数，因此是 1 或是 p 的倍数。但是

$$h_1+h_2+\cdots+h_t=p^m.$$

式中 $h_1=1$。所以至少还有另一个 $h_r=1\ (1<r\leqslant t)$。于是共轭类 C_r 由一个元素 a 组成。a 属于 G 的中心，所以 G 的中心大于 $\{e\}$。▎

定理10 p^2(p 是素数)阶群一定是交换群。

证明 设 G 是一个 p^2 阶群，如果 G 中有一个 p^2 阶元素，那么 G 是一个循环群。如果 G 不是循环群，那么 G 中非单位元素都是 p 阶元素。由定理8，$Z(G)\neq\{e\}$，取 $a\in Z(G)$，$a\neq e$，再取 $b\notin\langle a\rangle$。那么 $G=[a,b]$，所以 G 是交换的。▎

定理11 如果 p-群 P 只有一个指数为 p 的子群，那么 G 是一个循环群。

证明 设 $|P|=p^n$，对 n 作归纳法。

当 $n=1$ 时，结论显然成立。

设定理对阶为 $p^s(s<n)$ 的群都成立。用 Z 表示 G 的中心，如果 $|G:Z|=1$，则 G 是交换群，因此，G 是循环群。而且 $|G:Z|\neq p$，来证明 $|G:Z|\geqslant p^2$ 也不可能。如果 $|G:Z|=p^2$，则 G/Z 是 p^{s-2} 阶 p-群。如果 H/Z 是 G/Z 的指数为 p 的子群，那么 H 是 G 的指数为 p 的子群，因此由假设 G/Z 只有一个指数为 p 的子群，由归纳法假设，G/Z 为循环群，所以 G 是一交换群。与 $|G:Z|=p^2$ 相矛盾，所以只能有 $|G:Z|=1$，定理证毕。▎

§3 一些特殊 p-群

这节介绍一些特殊 p 群的构造而不加证明。

3.1 阶为 p,p^2,p^3 的群

(1) p 阶群

(i) 循环群 $\langle a\rangle$，$a^p=e$。

(2) p^2 阶群

(i) 循环群 $\langle a\rangle$，$a^{p^2}=e$。

(ii) 初等交换群 $\langle a,b\rangle$，$a^p=e$，$b^p=e$，$ba=ab$。

(3) p^3 阶群

交换群

(i) $\langle a\rangle$，$a^{p^3}=e$。

(ii) $\langle a,b\rangle$，$a^{p^2}=e$，$b^p=e$，$ba=ab$。

(iii) $\langle a,b,c\rangle$，

$$a^p=b^p=c^p=e,\quad ba=ab,\quad ca=ac,\quad cb=bc.$$

非交换群，$p=2$

(iv) 二面体群 $\langle a,b\rangle$，$a^4=b^2=e$，$ba=a^{-1}b$。

(v) 四元数群 $\langle a,b\rangle$，$a^4=e$，$b^2=a^2$，$ba=a^{-1}b$。

非交换群，$p\neq 2$

(iv′) $\langle a,b\rangle$，$a^{p^2}=e$，$b^p=e$，$b^{-1}ab=a^{1+p}$。

(v′) $\langle a,b,c\rangle$，

$a^p=b^p=c^p=e$，$ab=bac$，$ca=ac$，$cb=bc$。

3.2 包含指数为 p 的循环子群的 p^n 阶群

交换群

(1) $n\geqslant 1$

循环群$\langle a\rangle$，$a^{p^n}=e$。

(2) $n\geqslant 2$

$\langle a,b\rangle$，$a^{p^{n-1}}=e$，$b^p=e$，$ba=ab$。

非交换群

(3) p 为奇数，$n\geqslant 3$

$\langle a,b\rangle$，$a^{p^{n-1}}=e$，$b^p=e$，$ba=a^{1+p^{n-2}}b$。

(4) $p=2$，$n\geqslant 3$

广义四元数群$\langle a,b\rangle$，

$a^{2^{n-1}}=e$，$b^2=a^{2^{n-2}}$，$ba=a^{-1}b$。

(5) $p=2$，$n\geqslant 3$

二面体群$\langle a,b\rangle$，$a^{2^{n-1}}=e$，$b^2=e$，$ba=a^{-1}b$。

(6) $p=2$，$n\geqslant 4$

$\langle a,b\rangle$，$a^{2^{n-1}}=e$，$b^2=e$，$ba=a^{1+2^{n-2}}b$。

(7) $p=2$，$n\geqslant 4$

$\langle a,b\rangle$，$a^{2^{n-1}}=e$，$b^2=e$，$ba=a^{-1+2^{n-2}}b$。

3.3 关于p-群的其它结果

我们知道，只包含一个 p 阶子群的交换p-群一定是循环群，然而只包含一个 p 阶子群的非交换p-群也是存在的，例如四元数群就是一例，事实上，有下述结果。

定理12 只包含一个 p 阶子群的 p 群或者是循环群，或者是广义四元数群。

我们曾证明过，只包含一个指数为 p 的子群的p-群一定是循环群，更一般地，有

定理13 设$1<m<n$，则只包含一个 p^m阶子群的p^n阶群一定是循环群。

习　　题

1. 设H是G的一个正规子群，$|G:H|$与 p 互素，证明G的任一个 Sylow p-子群都包含在H中。

2. 设K是G的一个正规 p 子群，证明K包含于G的任一个 Sylow p-子群之中。

3. 证明：阶为 p^2q (p,q 为相异素数)的群一定不是单群。

4. H是G的子群，P 是H的 Sylow p-子群，证明：存在G的一个 Sylow p-子群Q使得

$$P=Q\cap H.$$

5. 设G包含一个指数为 p 的循环正规子群，证明G的任一子群也都有指数为 p 的循环正规子群。

6. 问：在168阶群中可能有多少个7阶元素？

7. 证明恰有 5 个不同构的12阶群。

8. 证明155阶群一定是循环群。

9. 证明546阶群一定是循环群。

10. 证明：阶为200的群一定不是单群。

11. 设$|G|=p^{a}\cdot n$，$(p,n)=1$。证明：如果G中恰有p^{a}个p元素，则G不是单群。

12. N是有限群G的一个正规子群，P是G的Sylow p-子群。求证：$P\cap N$是N的Sylow p-子群。

13. G,N,P同上题，试证：PN/N是G/N的Sylow p-子群。

14. 设p是非交换p-群，Z是P的中心，则$|P:Z|\geqslant 2$。

15. 设A是p群P的一个正规子群，$Z(P)$是P的中心。证明：$A\cap Z(P)\neq\{e\}$。

16. 如果置换群G的阶可被素数p整除，则G中一定有一个元素是不相交p-轮换的乘积。

17. 设p是一个素数，P是Ω上置换群G的一个Sylow p-子群，$\alpha\in\Omega$，证明：如果$p^{m}\,|\,|\alpha^{G}|$，则$p^{m}\,|\,|\alpha^{P}|$。

18. P,G,α的假设同上题，如果p^{m}是能整除$|\alpha^{G}|$的最高p幂，再设Δ是P在α^{G}中的最短传递集，则$|\Delta|=p^{m}$。

第六章 可 解 群

可解群是一类较常见的群。特别在证明了奇数阶群的可解性之后，可解群的构造在群论中更占有重要的地位。可解群在其它学科，特别在方程式论中也有重要的应用。

这一章主要介绍可解群的定义和有限可解群的一些判别条件。

在介绍可解群之前，先介绍次正规群列，正规群列，合成群列等概念。这些概念都是应用一些子群来讨论大群的重要工具。

最后一节介绍亚循环群、幂零群及超可解群的定义及有关结论。

§1 合 成 群 列

1.1 次正规群列

设G是一个群，H是G的一个非平凡正规子群：

$$G\triangleright H\triangleright\{e\}.$$

我们知道商群G/H是G的一个同态象，H是G到G/H的自然同态的核。因此，H与G/H的构造可以部分地反映G的构造。

如果H还有一个非平凡正规子群F：

$$H\triangleright F\triangleright\{e\},$$

那么我们又可以利用F与商群H/F来研究H。这样继续下

去，我们可以利用G的一系列子群及其商群来研究G。这就是所谓次正规群列的概念。

定义1 设G是一个群，$G_0,G_1,G_2,\cdots,G_s$是G的一些子群，满足

$$G=G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_s=\{e\}。\tag{1}$$

那么(1)称为G的一个**次正规群列**。G_i $(i=0,1,\cdots,s)$称为G的**次正规子群**。

如果每个G_i $(i=1,2,\cdots,s)$都是G的正规子群，那么(1)称为G的一个**正规群列**。

商群$G/G_1,G_1/G_2,\cdots,G_{s-1}/G_s$称为(1)的**因子**。因子的个数$s$称为(1)的**长度**。

例1 对于G的任一个正规子群H，

$$G \trianglerighteq H \trianglerighteq \{e\}$$

总是一个正规群列。

例2 设G是四元数群：

$$G=\langle a,b\rangle,\ a^4=e,\ a^2=b^2\neq e,\ ab=ba^3。$$

令

$$G_1=\langle a\rangle,\ G_2=\langle a^2\rangle。$$

则

$$G \triangleright G_1 \triangleright G_2 \triangleright \{e\}$$

是G的一个正规群列。

例3 $G=S_4$。令

$$G_1=\{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\},$$
$$G_2=\{e,(1,2)(3,4)\}。$$

则

$$G \triangleright G_1 \triangleright G_2 \triangleright \{e\}$$

是G的一个次正规群列但不是正规群列。

例4 用$G^{(1)}=G'$表示群G的换位子群，$G^{(2)}$表示$G^{(1)}$的换位子群，…，用$G^{(k+1)}$表示$G^{(k)}$的换位子群，那么对于任意正整数s，

$$G=G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq \cdots \trianglerighteq G^{(s)} \trianglerighteq \{e\}$$

是G的一个正规群列。

请读者自己证一下$G^{(k)} \trianglerighteq G$ $(k=1,2,\cdots,s)$。

在应用次正规群列来讨论群的构造时，这个群列的因子群起着重要的作用。因此我们需要下述定义。

定义2 设

$$G=G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_s=\{e\} \tag{2}$$

及

$$G=H_0 \trianglerighteq H_1 \trianglerighteq H_2 \trianglerighteq \cdots \trianglerighteq H_t=\{e\} \tag{3}$$

是群G的两个次正规群列。如果$s=t$而且可以在(2)与(3)的因子之间建立一个一一对应，使得对应的因子是同构的，那么我们就说(2)与(3)是**同构的**。

例5 G是S_6的一个18阶子群：

$$G=\{e,(1,2,3,4,5,6),(1,3,5)(2,4,6),(1,4)(2,5)(3,6),$$
$$(1,5,3)(2,6,4),(1,6,5,4,3,2),(1,3,5),$$
$$(1,2,5,6,3,4),(1,5,3)(2,4,6),(1,4,3,6,5,2),$$
$$(2,6,4),(1,6)(2,3)(4,5),(1,5,3),$$
$$(1,2)(3,4)(5,6),(2,4,6),(1,4,5,2,3,6),$$
$$(1,3,5)(2,6,4),(1,6,3,2,5,4)\}。$$

G的两个次正规群列

$$G \triangleright \{e,(1,3,5)(2,4,6),(1,5,3)(2,6,4),(1,3,5),$$
$$(1,5,3),(1,5,3)(2,4,6),(2,6,4),(2,4,6),$$
$$(1,3,5)(2,6,4)\}$$
$$\triangleright \{e,(1,3,5),(1,5,3)\} \triangleright \{e\}$$

及

$$G\rhd\{e,(1,5,3)(2,4,6),(1,3,5)(2,6,4),(1,4)(2,5)(3,6),$$
$$(1,6)(2,3)(4,5),(1,2)(3,4)(5,6)\}$$
$$\rhd\{e,(1,5,3)(2,4,6),(1,3,5)(2,6,4)\}\rhd\{e\}$$

的长度都是 3，它们的因子的阶分别是 2,3,3 及 3,2,3。因为阶为素数的群都是循环群，而且同阶的循环群一定是同构的，所以可以排列这两个次正规群列的因子，使得对应的因子同构。这说明这两个次正规群列是同构的。

还可以看出这两个次正规群列中，第一个不是正规群列，而第二个却是正规群列。

显然，次正规群列的同构关系是一个等价关系。

1.2 合成群列

为了能有效地应用次正规群列来研究一个群，我们希望这个次正规群列的因子越简单越好。从正规子群的角度来看，我们希望这些因子都是单群。那么，如何从 G 的一个正规子群 H 来判断 G/H 是否是单群呢？下述定理给出了一个条件。

定理1 商群 G/H 是单群的充分必要条件是 H 是 G 的一个极大正规子群。

证明 如果 H 不是 G 的极大正规子群，那么 G 有一个正规子群 F 使得

$$G\rhd F\rhd H.$$

于是 F/H 是 G/H 的一个非平凡正规子群，所以 G/H 不是单群。

反之，如果 G/H 不是单群。设 F/H 是 G/H 的一个非平凡正规子群。那么必有

$$G\rhd F\rhd H.$$

所以 H 不是 G 的极大正规子群。 ▎

于是我们可以引入下面的定义。

定义3 如果在 G 的无重复次正规群列

$$G=G_0\rhd G_1\rhd\cdots\rhd G_s=\{e\} \tag{4}$$

中，每个 $G_i(i=1,2,\cdots,s)$ 都是 G_{i-1} 的极大正规子群，那么(4)就称为 G 的一个**合成群列**。合成群列的因子称为 G 的**合成因子**。

在前面的一些例子中，例 2 中的正规群列是合成群列；例 3 中的正规群列则不是合成群列；例 5 中的两个次正规群列都是合成群列；而例 1 和例 4 则不一定。

当然，从定理 1 可以看出，一个无重复的次正规群列是合成群列的充要条件是每个因子都是单群。

有限群总是有合成群列的。而且，每个正规子群都可以作为某个合成群列中的一项；每个无重复的次正规群列都可以作为某个合成群列的一部分。这个事实可以这样来说明：设

$$G=G_0\rhd G_1\rhd G_2\rhd\cdots\rhd G_s=\{e\} \tag{5}$$

是有限群 G 的一个无重复的次正规群列。如果每个 $G_i(i=1,2,\cdots,s)$ 都是 G_{i-1} 的极大正规子群，那么(5)就是 G 的一个合成群列。如果 $G_l(1\leqslant l\leqslant s)$ 不是 G_{l-1} 的极大正规子群，那么可以找到 G_{l-1} 的一个正规子群 H 使得

$$G_{l-1}\rhd H\rhd G_l.$$

于是可以将 H 添入(5)中 G_{l-1} 与 G_l 之间而得到一个新的无重复的次正规群列

$$G\rhd G_0\rhd G_1\rhd\cdots\rhd G_{l-1}\rhd H\rhd G_l\rhd\cdots\rhd G_s=\{e\}, \tag{6}$$

如果这还不是一个合成群列，那么还可以用同样的方法在这

个次正规群列中添加一项，这样继续下去，由于 G 的有限性，最后总可得到一个合成群列。

次正规群列(6)称为(5)的一个加密。一般地，有下述定义：

定义4 设

$$G=G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_s=\{e\} \quad (7)$$

及

$$G=H_0 \trianglerighteq H_1 \trianglerighteq H_2 \trianglerighteq \cdots \trianglerighteq H_t=\{e\} \quad (8)$$

是群 G 的两个次正规群列。如果(7)的各项都包含在(8)中，就称(8)是(7)的一个**加密**。

显然，此时必有 $t \geqslant s$，上面所说的事实用这个定义来说就是

定理2 有限群的任一个无重复的次正规群列都可以加密成一个合成群列。

例如，例3中的次正规群列可以加密成一个合成群列

$$S_4 \triangleright A_4 \triangleright G \triangleright G_2 \triangleright \{e\}$$

值得注意的是，一个有限群可以有不止一个合成群列。例如，例5就给出同一个群的两个不同的合成群列。而且我们已经证明过这两个合成群列是同构的。读者可能在其它例子中遇到过同一个群的不同的合成群列，它们也都是同构的。于是不禁要问：这是不是一个一般的规律呢？下述定理给出了肯定的答案。这个定理是可以利用某个群的任一个合成群列来研究这个群的重要根据。

定理3(Jordan-Hölder) 有限群 G 的任两个合成群列都是同构的。

证明 我们对 G 的阶作归纳法来证明定理。

设

$$G=G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_s=\{e\} \quad (9)$$

及

$$G=H_0 \triangleright H_1 \triangleright H_2 \triangleright \cdots \triangleright H_t=\{e\} \quad (10)$$

是 G 的两个合成群列。

如果 $G_1=H_1$，则

$$G_1 \triangleright G_2 \triangleright \cdots \triangleright G_s=\{e\} \quad (9')$$

与

$$H_1 \triangleright H_2 \triangleright \cdots \triangleright H_t=\{e\} \quad (10')$$

是 G_1 的两个合成群列。因为 G_1 的阶小于 G 的阶，故由归纳法假设知(9′)与(10′)是同构的，从而(9)与(10)也是同构的。

如果 $G_1 \neq H_1$，则因 G_1 是 G 的一个极大子群，故 $G=G_1H_1$。任取 $G_1 \cap H_1=F_1$ 的一个合成群列：

$$G_1 \cap H_1=F_1 \triangleright F_2 \triangleright \cdots \triangleright F_r=\{e\}.$$

作 G 的次正规群列

$$G \triangleright G_1 \triangleright G \cap H_1 \triangleright F_2 \triangleright \cdots \triangleright F_r=\{e\} \quad (11)$$

及

$$G \triangleright H_1 \triangleright G \cap H_1 \triangleright F_2 \triangleright \cdots \triangleright F_r=\{e\}. \quad (12)$$

则因

$$G/G_1 \cong H_1/G_1 \cap H_1, \quad G/H_1 \cong G/G_1 \cap H_1$$

都是单群，所以(11)与(12)都是 G 的合成群列，而且是同构的。

又因 G_1，H_1 的阶都比 G 的阶小，所以由归纳法假设知(9′)(10′)分别与

$$G_1 \triangleright G_1 \cap H_1 \triangleright F_2 \triangleright \cdots \triangleright F_r=\{e\}$$

及

$$H_1 \triangleright G_1 \cap H_1 \triangleright F_2 \triangleright \cdots \triangleright F_r=\{e\}$$

同构。因此(9)与(11)，(10)与(12)分别同构。由同构关系的传递性知(9)与(10)同构。定理证毕。 ▎

这个定理说明：一个有限群的合成因子除次序外是唯一

确定的(在同构的意义下)，因此我们可以任取一个合成群列来进行讨论。

最后，我们给出定理 3 的一个推论。

定理4 有限群的任两个次正规群列都有同构的加密。

证明 如果这两个次正规群列都是无重复的，那么只要将它们加密到合成群列就可以应用定理 3 而得到结论。在有重复的情形，可以先将重复的项去掉而得到同构的加密，然后再在两个加密群列中同时添上重复的项。▎

当然，在具体应用时，有时不必加密到合成群列，可以针对具体的次正规群列来考虑。

§2 可 解 群

我们在前面曾介绍过，G 的换位子群 G' 是 G 的一个正规子群，其商群 G/G' 是一个交换群，用 G'' 表 G' 的换位子群，…，用 $G^{(k+1)}$ 表 $G^{(k)}$ 的换位子群，这样可以得到一系列子群

$$G \trianglerighteq G' \trianglerighteq G'' \trianglerighteq \cdots \trianglerighteq G^{(k)} \trianglerighteq G^{(k+1)} \trianglerighteq \cdots.$$

对于有限群来说，总有某个正整数 s 使得

$$G^{(s)} = G^{(s+1)} = \cdots.$$

有两种可能：或者 $G^{(s)} = \{e\}$，或者 $G^{(s)} \neq \{e\}$。满足 $G^{(s)} = \{e\}$ 的群称为可解群。

定义5 如果有正整数 s 使得 $G^{(s)} = \{e\}$，那么 G 称为**可解群**。

例1 交换群都是可解群。

例2 四元数群是可解群。

例3 S_n 及 A_n $(n>4)$ 都不是可解群。

证明 已知当 $n>4$ 时，S_n 只有一个非平凡正规子群，即 A_n，而 A_n 是一个单群。

因为 S_n 的换位元素都是偶置换，所以 $S_n' \neq S_n$，但是 S_n 不是交换群，因此 $S_n' \neq \{e\}$。这两点说明 S_n' 是 S_n 的非平凡正规子群。所以 $S_n' = A_n$。

$A_n (n>4)$ 不是交换群，所以 $A_n' \neq \{e\}$。由 A_n 的单性，知 $A_n' = A_n$。▎

请读者自己验证一下 S_3 及 S_4 都是可解群。

因为，对群 G 的子群 H，总有 $G^{(i)} \geqslant H^{(i)}$，所以可解群的子群也是可解的，不但如此，可解群的商群也是可解的。

定理5 可解群的子群和商群都是可解的。

证明 只要对商群来证明。如果 H 是 G 的一个正规子群，那么商群 $Q = G/H$ 是 G 的一个同态象。因此，$Q^{(i)}$ 是 $G^{(i)}$ 的同态象。于是从 $G^{(s)} = \{e\}$ 可推出 $Q^{(s)} = \{e\}$。▎

定理6 可解单群一定是素数阶循环群。

证明 由 G 的可解性知 $G' \neq G$，再由 G 的单性得 $G' = \{e\}$。所以 G 是一个交换群。我们已知交换的单群一定是素数阶循环群。▎

下面给出可解群的几个充分必要条件。

定理7 对于有限群 G，下面几个条件都是等价的。

(1) G 是一个可解群。

(2) G 有一个正规群列，其因子都是交换的。

(3) G 有一个次正规群列，其因子都是交换的。

(4) G 的合成因子都是素数阶循环群。

证明 (1)⇒(2)。当 G 可解时，G 的换位子群列就是一个正规群列，其因子都是交换的。

(2)⇒(3)。因为凡是正规群列一定是次正规群列，所以

从(2)可推出(3)。

(3)⇒(4)。设

$$G=G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_s=\{e\}$$

是G的一个次正规群列，因子$G_{i-1}/G_i(i=1,2,\cdots,s)$都是交换的，来证明$G$的合成因子都是素数阶循环群。为了方便起见，可设这个群列是无重复的。

对G的阶作归纳法。

取G的包含G_1的一个极大正规子群H_1，则G/H_1是一个单群，而且是交换的，所以G/H_1一定是一个素数阶循环群。

$$H_1 \trianglerighteq G_1 \triangleright G_2 \triangleright \cdots \triangleright G_s=\{e\}$$

是H_1的一个次正规群列，其因子都是交换的，因为H_1的阶比G的阶小，故由归纳法假设，H_1的合成因子都是素数阶循环群。设

$$H_1 \triangleright H_2 \triangleright \cdots \triangleright H_t=\{e\}$$

是H_1的一个合成群列，那么

$$G \triangleright H_1 \triangleright H_2 \triangleright \cdots \triangleright H_t=\{e\}$$

是G的一个合成群列，所以G的合成因子也都是素数阶循环群。

(4)⇒(1)。设

$$G=G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_s=\{e\}$$

是G的一个合成群列，其因子都是素数阶循环群，因为G_{i+1}/G_i是交换的，故必有

$$G_1 \geqslant G',\ G_2 \geqslant G_1' \geqslant G'',\cdots,G_i \geqslant G^{(i)},\cdots,G_s \geqslant G^{(s)}.$$

现在$G_s=\{e\}$，所以$G^{(s)}=\{e\}$，G是可解的。▎

推论 如果群G有一个可解正规子群H，使得商群G/H是可解的，那么G也是可解的。

证明 如果

$$H \triangleright H_1 \triangleright \cdots \triangleright H_{s-1} \triangleright \{e\}$$

及

$$G/H \triangleright G_1/H \triangleright \cdots \triangleright G_{t-1}/H \triangleright H/H$$

分别是H及G/H的次正规群列，它们的因子群都是交换的，那么

$$G \triangleright G_1 \triangleright \cdots \triangleright G_{t-1} \triangleright H \triangleright H_1 \triangleright \cdots \triangleright H_{s-1} \triangleright \{e\}$$

就是G的一个次正规群列，其因子也都是交换的。▎

根据第五章定理5推论2，我们有下述结论。

定理8 有限p群是可解群

证明 设G是一个p^m阶群，则G有一个次正规群列

$$G_0=G \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_m=\{e\}.$$

其中$G_i(i=1,2,\cdots,m)$是p^{m-i}阶群。于是G_{i-1}/G_i $(i=1,2,\cdots,m)$是p阶循环群，所以G是可解的。▎

下面的两个定理说明可解群是一类很广的有限群。

定理9(Burnside) 阶为$p^a q^b$(p,q为素数，a,b为自然数）的群一定是可解的。

定理10(Feit-Thompson) 奇数阶群是可解群。

定理9通常称为$p^a q^b$定理，是Burnside首先应用群指标的理论证明的。近年来，虽然有一些纯群论的证明，但是都非常复杂。至于定理10，Feit-Thompson两人原来的证明长达二百多页，虽经多次改进，其证明仍可成为一本专著，这两个定理的证明都超出了本书的范围，应用定理9可以证明可解群的一个充分条件。

定理11 如果有限群G的所有极大子群的指数都是素数或素数的平方，那么G是可解的。

证明 对G的阶进行归纳法，设结论对阶比$|G|$小的群都成立。

设p是整除$|G|$的最大素数，P是G的一个Sylow p-子群。用N表示P在G内的正规化子。如果$N=G$，那么P是G的正规子群，商群G/P的极大子群的指数也是素数或素数的平方。因为G/P的阶比G的阶小，故由归纳法假设，G/P是可解的，P是一个p-群，故由定理8，P是可解的，再应用定理7的推论，即可得G的可解性。

如果$N\neq G$，设H是G的包含N的一个极大子群，P在H内的正规化子也就是N，故由第二Sylow定理，

$$|G:N|=1+k_1p,\ |H:N|=1+k_2p.$$

因此
$$|G:H|=1+kp.$$

由假设，H在G内的指数等于某个素数q或q^2。由p是$|G|$的最大素因数，推出$|G:H|=q^2$，于是

$$kp=q^2-1=(q-1)(q+1).$$

由于$p>q$，故必有$p=q+1$。因此必须有$p=3$，$q=2$。于是$|G|=2^a3^b$，由定理9，知G是可解群。▌

最后我们介绍关于可解群的推广的Sylow定理。我们以前证明了Sylow定理：如果G的阶等于p^an，p是素数，$(p,n)=1$，那么G一定有p^a阶子群，称为Sylow p-子群；G的Sylow p-子群都是共轭的；G的Sylow p-子群的个数h是$|G|$的一个因数而且模p同余于1。对于可解群，这个结论可以推广，我们将关于可解群的推广的Sylow定理叙述在下面而不作证明。

定理12 设G是一个可解群，G的阶为mn，$(m,n)=1$，则

(1) G有m阶子群。

(2) G的m阶子群都是共轭的。

(3) G的任一个阶为m的因数的群一定包含在G的某个m阶子群之中。

(4) G的m阶子群的个数h_m可以表成一些因数之积，而使每个因子满足：

(a) 模m的某个素因子同余于1；

(b) 是一个素数的方幂。

定理12中的第(1)点事实上也是可解群的一个特征性质，为了叙述这一结论，要用到一个定义：如果G的阶为p^an，$(n,p)=1$，那么G的n阶子群称为G的一个p-补群。

定理13 如果对$|G|$的每个素因子p，G都有p-补群，那么G是一个可解群。

§3 亚循环群、幂零群和超可解群

这一节介绍亚循环群、幂零群及超可解群的定义及它们的一些重要性质。

定义 6 如果群G的导群G'和商群G/G'都是循环群，则称G为**亚循环群**。

如果G是亚循环群，那么$G''=\{e\}$，所以G是可解的。

定理14 如果有限群G的Sylow子群都是循环群，那么G一定是亚循环群，并且G可以由两个元素a,b生成，a,b满足下述关系：

$$a^m=e,\ b^n=e,\ b^{-1}ab=a^r,$$

$$mn=|G|,\ ((r-1)n,m)=1,\ r^n\equiv 1 \pmod{m}.$$

反之，如果群G由满足上述关系的元素a,b生成，那么G的Sylow子群一定都是循环群，因之G是亚循环群。▌

因为亚循环群一定是可解的，所以定理14给出可解群的一个充分条件。

推论 如果群G的Sylow子群都是循环群，那么G是可解的，特别地，如果群G的阶是一些相异素数的乘积，那么G是可解的，并且还是循环的。▎

定义 7 设G是一个群。

$$G=G_0\trianglerighteq G_1\trianglerighteq G_2\trianglerighteq\cdots\trianglerighteq G_s=\{e\}$$

是G的一个正规群列。如果G_{i-1}/G_i包含在G/G_i的中心内($i=1,2,\cdots,s$)，则称这个群列为G的一个**中心群列**。具有中心群列的(有限)群称为**幂零群**。

因为上述定义中G_{i-1}/G_i是交换的，所以幂零群一定是可解的。

定义 8 设G是一个群。令

$\Gamma_1(G)=G$，$\Gamma_k(G)=\langle[x_1,\cdots,x_k]\rangle$ (x_i为G的任意元)。

则有

$$\Gamma_{k+1}(G)\triangleleft\Gamma_k(G),\qquad k=1,2,\cdots.$$

群列

$$G=\Gamma_1(G)\trianglerighteq\Gamma_2(G)\trianglerighteq\Gamma_3(G)\trianglerighteq\cdots$$

称为G的**下中心群列**。

定义 9 设G是一个群。

$$Z_0=1\leqslant Z_1(G)\leqslant Z_2(G)\leqslant\cdots\leqslant Z_i(G)\leqslant Z_{i+1}(G)\leqslant\cdots$$

是G的一个子群列。如果$Z_{i+1}(G)/Z_i(G)$是$G/Z_i(G)$的中心，则称此群列是G的**上中心群列**。

如果

$$G=A_1\trianglerighteq A_2\trianglerighteq A_3\trianglerighteq\cdots\trianglerighteq A_{r+1}=1$$

是群G的一个中心群列，那么

$$A_i\geqslant\Gamma_i(G),\qquad i=1,2,\cdots,r+1;$$

$$A_{r+1-j}\leqslant Z_j(G),\qquad j=0,1,\cdots,r.$$

因此，如果G有长度有限的中心群列，那么G的上、下中心群列都是有限的，是特殊的中心群列，并且有下述结论。

定理15 如果G是一个幂零群，那么G的上、下中心群列都是有限长的，且有等长c。

定理15中的c称为幂零群G的类。

下面我们介绍幂零群的性质而不予证明。

定理16 幂零群的子群及商群都是幂零群。

定理17 (1) 幂零群的每个真子群的正规化子都不能等于这个子群。

(2) 幂零群G的每个极大子群都是正规的，其指数为奇数，而且包含G的导群。

(3) 若H是幂零群G的子群且$G=G'H$，那么$H=G$。

定理18 有限p-群是幂零群。有限群G是幂零群当且仅当G可表成它的Sylow子群的直积。

推论 有限群是幂零的当且仅当它的极大子群都是正规的。

我们介绍群的一类幂零子群。

定义10 群G的所有极大子群之交称为G的Frattini子群，记作$\Phi(G)$。

定理19 (1) 有限群的Frattini子群是幂零的。

(2) 有限群G是幂零群的充分必要条件是$\Phi(G)\geqslant G'$。

定义11 如果群G有一个次正规群列

$$G=G_0\trianglerighteq G_1\trianglerighteq G_2\trianglerighteq\cdots\trianglerighteq G_s=\{e\},$$

其中每个商群G_{i-1}/G_i ($i=1,2,\cdots,s$)都是循环群，则G叫做**超可解的**。

由定义可看出超可解群一定是可解的。超可解群有下述一些性质。

定理20 超可解群的子群和商群都是超可解群。超可解群的导群是幂零的。

定理21 有限群G是超可解群的充分必要条件是G的极大子群的指数都是素数。

习　题

1. 找出20阶循环群的所有可能的合成群列。

2. 证明S_3,S_4都是可解群。

3. 设H是G的一个同态象，N是G到H的某个同态映射的核，证明：

(1) 如果G是可解群，则H也是可解的。

(2) 如果H是可解群，则当且仅当N可解时G是可解的。

4. 证明可解群的直积也是可解群。

5. 证明pq (p,q是素数)阶群是可解群。

6. 证明p^2q (p,q是不同素数)阶群是可解群。

7. 证明如果G的 Sylow 2-子群是循环群，那么G是可解群。

8. 证明：$A\lhd\lhd G$，$B\lhd\lhd G\rightarrow\langle A,B\rangle\lhd\lhd G$ ($A\lhd\lhd G$表示A是G的次正规子群)。

9. 证明：有限群G是幂零群的充分必要条件是G的子群都是次正规的。

10. 如果u是一个奇数，则$2u$阶群一定是可解的。

11. 设M,N都是群G的正规子群。证明：如果G/M，G/N都是幂零的，那么G也是幂零的。

12. 设G是有限交换群，$|G|=p_1^{n_1}p_2^{n_2}\cdots p_r^{n_r}$，其中$p_1,\cdots,p_r$是不同素数，那么$G$的合成群列的长等于$\sum_{i=1}^{r}n_i$。

13. 设$Z(G)$是G的中心，$A\leqslant Z(G)$。试证：如果G/A是幂零群，则G也是幂零群。

14. 证明：非交换可解群G的换位子群G'不可能是G的直积因子。

15. 证明：非交换幂零群G的中心不能作为G的直积因子。

16. 证明：非交换群G为2类幂零群的充要条件是

$$G'\leqslant Z(G)\ (Z(G)\text{是}G\text{的中心})。$$

17. 设$G=G_0\trianglerighteq G_1\trianglerighteq G_2\trianglerighteq\cdots\trianglerighteq G_l=1$是$G$的一个中心群列，$H$是$G$的一个子群。试证：如果$H\geqslant G_i(1\leqslant i\leqslant l)$，则$H$的正规化子$N_G(H)\geqslant G_{i-1}$。

18. 设$N\trianglelefteq G$，$H\leqslant G$，且$N\leqslant\Phi(H)$，则$N\leqslant\Phi(G)$。

19. 证明从$N\trianglelefteq G$可推出$\Phi(N)\leqslant\Phi(G)$。

20. 设G/N是超可解群，N是循环群，证明G是超可解群。

复 习 题

1．$a_1,a_2,\cdots,a_n$ 是群G中 n 个元素，证明：$a_1a_2\cdots a_n$与 $a_r\cdots a_na_1\cdots a_{r-1}$ $(2\leqslant r\leqslant n)$共轭，因而它们的阶相等。

2．证明：在阶大于 2 的群中，存在元素a,b，a与 b 都是非单位元素，且$a\neq b$，使$ab=ba$。

3．A,B是群G的子群，a,b 是群G的元素，证明：如果$Aa=Bb$，则$A=B$。

4．如果K是群G的一个子集，用 K^{-1} 表示由K中每个元素的逆元素组成的子集：

$$K^{-1}=\{a^{-1}\mid a\in K\}.$$

证明：如果K是G的子群H的一个右陪集，则K^{-1}是H的一个左陪集。

5．证明：如果 $a_1,a_2,\cdots,a_r$是G的子群 H 在G中的一个右陪集代表系，那么 $a^{-1},a_2^{-1},\cdots,a_r^{-1}$是$H$在$G$中的一个左陪集代表系。

6．设A与B是群G的两个子群。证明：如果A与B的并集$A\cup B$是G的一个子群，那么必有$A\leqslant B$或$B\leqslant A$。

7．设G是一个pq阶群，p,q 都是素数且 $p<q$，则G的 q 阶子群是G的特征子群。

8．证明每个循环群都是无限循环群的同态象。

9．H是G的一个指数为 r 的子群，a 是G的一个中心元素，则$a^r\in H$。

10．设A是G的一个极大交换子群，则$Z_G(A)=A$。

11．设A是G的一个交换子群，且对A中任一元素$a\neq 1$都有$Z_G(a)=A$，则对G中任一元素 x 都有

$$x^{-1}Ax=A\text{或 }x^{-1}Ax\cap A=\{e\}.$$

12．证明：不同构的 4 阶群共有二个，作出它们的乘法表。

13．证明：如果G有一个指数为 4 的正规子群，那么G一定有指数为 2 的正规子群。

14．设G是一个单群，G的阶不等于 2，φ 是G到群H上的一个同态映射。证明：如果H有一个指数为 2 的正规子群A，那么$G^\varphi\leqslant A$。

15．设A是G的一个正规子群，G/A是奇数阶有限群。证明：G中满足$a^2=e$的元素 a 都在A中。

16．证明：如果 $H\trianglelefteq G$且$(|H|,|G:H|)=1$，则 H 是G的特征子群。

17．设M是单群G的一个极大子群，则$N_G(M)=M$。

18．设A是G的特征子群，B是G的子群，B/A 是G/A的特征子群，那么B是G的特征子群。

19．设 φ 是群G的一个自同构，并设对G中任意元素 a 都有$a^{-1}a^\varphi\in Z(G)$。试证：对G'中任一元素 b 都有 $b^\varphi=b$。

20．设$a_1,a_2,\cdots,a_n$是群G中 n 个元素，$i_1,i_2,\cdots,i_n$是1，2，…，n的一个排列。求证：$a_1a_{i_1}^{-1}a_2a_{i_2}^{-1}\cdots a_na_{i_n}^{-1}\in G'$

21．证明：在 n 次对称群中，阶为奇数的置换必为偶置换。

22．证明：

$$S_n=\langle(1,2),(1,3),\cdots,(1,n)\rangle$$
$$=\langle(1,2),(1,2,\cdots,n)\rangle,$$
$$A_n=\langle(1,2,3),(1,2,4),\cdots,(1,2,n)\rangle.$$

23．证明：S_n 中一个置换 σ 是一个换位元素的充分必要条件是 σ 可以表成两个同型置换之积。

24．验证下列等式：

$$(1,2,\cdots,2k+1)=(k+1,k+2,\cdots,2k+1)(1,2,\cdots,k+1);$$

$$\begin{aligned}(1,2,\cdots,2k)&(2k+1,2k+2,\cdots,2k+2l)\\&=(2k,k+l+1,k+l+2,\cdots,2k+2l)\\&\quad\times(1,2,\cdots,2k,2k+1,\cdots,k+l+1)(k\leqslant l)\end{aligned}$$

25． 证明$S_n'=A_n$，而且A_n中元素都是S_n的换位元素。

26．证明$\{1,2,3,4,5\}$上的置换群

$$\langle(1,2,3,4,5),(2,3,5,4),(1,6)(3,4)\rangle$$

是一个 3 重传递群，其阶为120。

27．证明：$\langle(1,2,3,4,5,6,7),(2,6)(3,4)\rangle$ 是一个 168 阶单群。

28．设G是一个正则群。证明：当且仅当$|G|$是一个素数时，G是本原的。

29．证明：如果本原群G的次数是一个大于 2 的偶数，那么G的阶可被 4 整除。

30．G是S_n的一个半正则子群，证明G在S_n内的中心化子是传递的。

31．G是一个有限交换群，对G中任意元素 a 都有$a^d=e$ 的最小正整数 d 称做G的指数。证明G中有 d 阶元素。

32． G是 n 阶交换群，证明：G是循环群$\rightleftharpoons G$的指数为 n。

33．证明：（1）有限域的乘法群是循环群。

（2）任一域的乘法群的有限子群是循环群。

34．证明：（1）交换 p 群G的初等交换子群都包含在G_p中。

（2）如果G的不变量为$p^{n_1},p^{n_2},\cdots,p^{n_r}$，则$G$共有$p^r-1$个 p 阶元素。

35．证明：p^r阶初等交换群的自同构群的阶为

$$p^{\binom{r}{2}}(p^r-1)(p^{r-1}-1)\cdots(p-1).$$

36．证明：p^r阶初等交换群的p^m阶子群的个数为

$$\frac{(p^r-1)(p^{r-1}-1)\cdots(p^{r-m-1}-1)}{(p^m-1)(p^{m-1}-1)\cdots(p-1)}.$$

37．证明：如果交换p群G的不变量为$p^{n_1},p^{n_2},\cdots,p^{n_r}$，则$G$的$p^m$阶初等交换子群的个数同上题。

38．设G的阶为 $p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s}$（$p_1,p_2,\cdots,p_s$ 为不同素数）。证明G为交换群的充分必要条件为：G有指数为$p_i^{k_i}$（$i=1,2,\cdots,s$）的交换正规子群。

39．已知有限群G中恰有一半元素的阶都是 2，而另一半元素组成的G的一个子群H，试证H是一个奇阶交换群。

40．证明：p^2阶非循环群是两个 p 阶循环群的直积。

41． p 是一个素数， 证明 S_p 有$(p-1)!$ 个 p 阶元素，$(p-2)!$个 p 阶子群。

42． p 是一个素数，$p<n<2p$，问S_n有多少个 p 阶元素，多少个 p 阶子群？如果 $n=2p$呢？

43．证明：p^2q^2（p,q为相异素数）阶群必可解。

44．证明：p^2qr（p,q,r 为相异素数）阶群或为可解群或与60阶单群A_5同构。

45．证明30阶群一定是可解群。

46．找出全部互不同构的30阶群。

47．如果p-群P有一个指数为p^2的交换子群，则P必有指数为p^2的正规交换子群。

48. 如果有限群G的每个极大子群都是单群，且在G中正规，那么G是交换群。

49. 用$I^{(1)}(G)$表示群G的内自同构群，$I^{(2)}(G)$表示$I^{(1)}(G)$的内自同构群，一般地用$I^{(k+1)}$表示$I^{(k)}$的内自同构群。证明：G是幂零群的充分必要条件是存在一个正整数n使$G^{(n)}$为单位群。

50. 设a, b是有限幂零群G中的两个元素。证明：如果a, b的阶互素，那么$ab=ba$。

51. 设G是可解群，$|G|=mn$，$(m,n)=1$，m_1是m的一个因数。证明：如果H是G的一个m_1阶正规子群，那么H一定是G的任一个m阶子群的正规子群。

52. 设G为有限幂零群，G/G'为循环群，证明G是循环群。